Under pressure: Understanding the dynamics of coordination in IT functions under business-as-usual and emergency conditions

Kotlarsky, Julia; van den Hooff, Bart; Geerts, Leonie

published in
Journal of Information Technology
2020

DOI (link to publisher)
10.1177/0268396219881461

document version
Publisher's PDF, also known as Version of record

citation for published version (APA)
Kotlarsky, J., van den Hooff, B., & Geerts, L. (2020). Under pressure: Understanding the dynamics of coordination in IT functions under business-as-usual and emergency conditions. *Journal of Information Technology*, *35*(2), 94-122. https://doi.org/10.1177/0268396219881461

JIT

Research Paper

Journal of Information Technology
2020, Vol. 35(2) 94–122

DOI: 10.1177/0268396219881461
Journals.sagepub.com/jinf
SAGE

Under pressure: Understanding the dynamics of coordination in IT functions under business-as-usual and emergency conditions

Julia Kotlarsky[1], Bart van den Hooff[2] and Leonie Geerts[3]

Abstract

In an era when technologies have become a backbone of most organizations, IT support functions are under immense pressure not only to ensure provision and reliability of IS and technologies but also to resolve IS incidents of different severity when they disrupt organizations' "business-as-usual." This article addresses this challenge by investigating how organizational IT functions coordinate their work under different degrees of uncertainty in order to provide reliable IT services. We conceptualize coordination in IT support functions as a process that unfolds over time through interactions between four underlying coordination practices employed to provide reliable IT services: prioritizing tasks, following procedures, using roles and responsibilities, and utilizing networks. Furthermore, we show how these coordination practices change when IT incidents cause a shift from normal (i.e. "business-as-usual") to emergency conditions. Our empirical research in two IT functions supporting two types of organizations (traditional and fast-response) demonstrate that IT functions in these two types of organizations respond to emergencies differently. Specifically, in emergencies, an IT function supporting a fast-response organization shifts to emergency coordination practices momentarily, as it abandons "normal" coordination practices to rely on an extensive set of formal practices specifically designed for such situations. In contrast, an IT function supporting a traditional organization is unprepared for emergencies—coordinating under emergency conditions involves improvisation, because coordination practices designed to support business-as-usual are not suitable for dealing with emergency situations.

Keywords

IT support function, coordination, IS incident, emergency, traditional organization, fast-response organization, military

Introduction

On May 12th 2017, business-as-usual in the National Health Services (NHS) in the UK was suddenly disrupted as IT systems in several hospitals and medical centers across the UK were attacked by so called "ransomware" that blocked access to any files until a ransom was paid.[1] Affected hospitals canceled all operations, ambulances were diverted to A&E in other, not affected, hospitals. In the following days the impact of this cyber attack on the NHS was evident among many institutions and businesses in the UK. For example, in the afternoon of May 12th, the IT department of a University released a message to all staff warning them about this ransomware attack and announcing measures to protect the University. On May 15th, staff in a local supermarket was constantly apologizing to customers about till systems being very slow, and not being able to process "click and collect" orders: "I cannot scan the parcel, the system is just not loading, because of this IS incident" a staff member commented. On May 16th, the Headmaster of a local school emailed all parents that, as a preventive measure, all external emails having attachments would be automatically removed and that updated security software would be implemented shortly.

[1]The University of Auckland, New Zealand
[2]Vrije Universiteit Amsterdam, The Netherlands
[3]Logius, The Netherlands

Corresponding author:
Julia Kotlarsky, The University of Auckland, 12 Grafton Street, Auckland 1010, New Zealand.
Email: j.kotlarsky@auckland.ac.nz

This example brings to fore the role of the Information Technology (IT) support function in enabling organizations to restore their business after this has been disrupted by a severe IT-related incident. Today, organizations' dependence on IT (and therefore on the IT support function) is immense: medical doctors cannot operate without access to patient information, which may be a case of life or death for some patients; retail business is disrupted by slow systems, schools and universities cannot function in their usual way until their IT support function is able to restore access to systems and ensure that security measures are in place. Hence, these incidents create increased levels of uncertainty about the availability and reliability of IT services, suddenly making the typically "invisible" IT support function the focal point of attention, as organizations' ability to go back to normal depends on it. In this article, we focus on this increasingly important role of the IT function in organizations and analyze how the IT function coordinates interdependent tasks and actors in order to realize a collective performance in terms of restoring a reliable provision of IT services that meet business requirements after an IT-related incident.

While the reliability of IT (Butler and Gray, 2006) and the role of the IT support function in organizations (Guillemette and Paré, 2012; Peppard, 2003, 2018; Sambamurthy and Zmud, 2000; Tarafdar and Tanriverdi, 2018) have been studied by Information Systems (IS) scholars, to the best of our knowledge researchers have not considered the dynamic nature of work in an IT support function to reflect how work is coordinated in this function in response to incidents that create uncertainty about this reliability. Given the impact of IT-related incidents on organizations, it seems imperative to understand how IT support functions respond to such incidents by effectively coordinating work in order to be able to reliably provide IT services under different degrees of uncertainty. As incidents concern a *change of state* in an IS (typically from a desired to an undesired state) (Baskerville et al., 2014), it is to be expected that in order to be able to respond to this, the IT function will also have to change the way it coordinates its work in order to restore reliable IT services. Therefore, our interest is in how coordination of work in the IT function changes in response to IT-related incidents.

Disruptions of IT services might be triggered by multiple factors. For instance, there can be external triggers such as the Egyptian revolution of 2011 that led to a shutdown of the Internet in Egypt and meant that some multinationals experienced service disruptions, having to evacuate expatriates to their home countries. Internal factors such as an acquisition or appointment of a new top executive also often trigger IT-related organizational change (e.g. the need to integrate IT systems of two merging organizations and transform the way back-offices provide IT-enabled services, or offshoring an IT-enabled business processes). Some of these triggers may not be immediate, allowing the IT support function to prepare for the change (e.g. to plan an enterprise system implementation as a phased approach; Umble et al., 2003), while others, like in the case of the ransomware attack, would be considered as an *emergency* and would require immediate action from the IT support function in response to a sudden increase in uncertainty about the provision of IT services. The earlier example of the impact of a ransomware attack is shedding light onto how IT support functions of some organizations are responding to particular emergency situations. In this example, their responses varied from "24/7 focusing on resolving the issue" (in NHS), to issuing a warning (in the university) and finding a creative temporary solution such as removing all attachments (at the school).

Looking beyond this specific example toward theory-building, these observations warrant further research into, and theorizing about, how organizational IT functions coordinate their work under different degrees of uncertainty in order to provide reliable IT services. Our study focuses on how the coordination practices that IT functions employ to provide reliable IT services change when IT incidents cause a change from normal (i.e. "business-as-usual") to emergency conditions. We conceptualize IT functions' responses to an emergency as a "shift" of coordination practices and analyze how such a shift actually happens, leading to a change in coordination practices employed under different levels of uncertainty. Hence, our research question is "How does coordination in IT support functions change in response to emergency situations?"

This research makes a unique contribution to the IS literature by theorizing coordination in the IT support function as a dynamic process that changes as this function is confronted with emergency conditions. Furthermore, we specifically study this change in two types of organizations: traditional and fast-response. Our study demonstrates that while there is a single baseline depicting coordination in both IT support functions under normal operating conditions, IT functions in two different types of organizations respond to emergencies differently, which is captured in the process view. Our results indicate that, in emergencies, an IT function supporting a fast-response organization shifts to emergency coordination practices momentarily, as it abandons "normal" coordination practices to rely on an extensive set of formal practices specifically designed for such situations. In contrast, for an IT function supporting a traditional organization, this shift is taking longer and coordinating under emergency conditions involves improvisation, because coordination practices designed to support business-as-usual are not suitable for dealing with emergency situations.

Theoretical background

The increasing globalization and digitization the world is witnessing today is manifested in the extensive reliance on

information technologies which we experience on the individual, organizational, and societal levels. The complexity and rate of development of digital technologies make it increasingly difficult to predict the behavior of these technologies and make organizations increasingly vulnerable to technological incidents that fundamentally affect them. As Butler and Gray (2006) put it, "individuals, organizations, and societies increasingly depend on information systems to reliably provide core services and capabilities" (p. 211), which highlights reliability as a central concern of the IT support function across a wide range of organizations (Guillemette and Paré, 2012).

The IT support function is responsible for the reliable provision of a broad and dynamically changing range of services concerning the processing, provisioning, and stewardship of information (Peppard, 2003), including hardware and software selection and installation, building and managing an IT infrastructure, coordination of IT-based projects, systems development and maintenance, user support, and leading digital innovation initiatives (Guillemette and Paré, 2012; Jia and Reich, 2013; Kettinger and Lee, 1994; Tarafdar and Tanriverdi, 2018). In order to be able to deliver those services, the interdependent tasks of various people and sub-units that are part of the IT function need to be coordinated—from development to maintenance, from operations to project management, etc. For any IT function, coordinating work to ensure the reliable provision of IT systems and services is a daunting endeavor—especially when having to respond to increasingly frequent and severe disruptions, as we elaborate in the next section.

IT incidents, business-as-usual, and emergencies

IT functions are increasingly confronted with IT incidents in the form of "discrepant IT events" (de Guinea and Webster, 2013). IT incidents are defined as "a change of state in a bounded information system from the desired state to an undesired state" or "an event that evades any preventative controls [. . .] and inflicts negative changes on information systems" (Baskerville et al., 2014: 139). Incidents, for instance, can be operational failures in hardware, software, or networks, or security and privacy incidents. Such incidents can disrupt business-as-usual, putting pressure on the IT support function.

The extent to which business-as-usual is interrupted by such incidents is partly determined by the gravity of the incident, but also by the nature of the organization that a particular IT function is supporting. Going back to the opening example of the ransomware attack, the IT function in the NHS (which is supporting hospitals across the United Kingdom) was put under enormous pressure to resolve the situation, because it presented a matter of life or death for many patients. On the other hand, for the IT function of the food retail chain, this incident was potentially related to the loss of revenue (as a result of tills being slow), but it did not endanger human lives. Therefore, IT functions in high uncertainty environments (e.g. hospitals, fire brigades, police) are typically expected to act as a fast-response organization themselves, as they are required to respond to a disruption immediately, flexibly and without room for error, resolving the incident so that the organization could return back to normal operating conditions. Furthermore, in fast-response organizations, the IT support function is expected to support urgent IT-related requests related to a specific mission or operation, which are typically associated with life-threatening urgency and unexpected events, requiring organizations to operate under time constraints and confused inputs (Schakel et al., 2016) and have low tolerance to mistakes.

When put under pressure, the conditions associated with emergency (high uncertainty, fast decision making, mistakes can be catastrophic) are also valid for the IT support function in traditional (i.e. non fast-response) organizations when business-as-usual is disrupted. A bank, for instance, can be confronted with an emergency if the electronic banking system is being hacked, threatening the integrity of customer and transaction data and ultimately the organization's survival. Conversely, a fast-response organization is not always in an emergency mode: even fire fighters, SWAT teams, A&E physicians, and military personnel have routine processes and procedures guiding the non-emergency part of their day-to-day work. Hence, in both traditional and fast-response organizations, we will find normal operating conditions and emergency operating conditions.

Normal operating conditions entail internal and external environmental conditions that an organization is prepared and designed for, based on past experience and predictable future changes. Such conditions would constitute business-as-usual for the organization, characterized by generally low levels of uncertainty. *Emergency operating conditions* are experienced when the organization is facing a situation that (1) contains pervasive uncertainty (i.e. incidents that do not fit routine procedures); (2) creates pressure for quick execution (e.g. the need to avoid delays in the case of a film production crew (Bechky and Okhuysen, 2011), or the need to directly repair a data leak at a security agency); and (3) can have negative consequences such as additional costs (e.g. loss of customers for a web shop that was hacked) or creates a danger of severe physical harm (e.g. for members of a SWAT team and people close to the place where the mission is taking place). Whenever an IT incident creates such conditions, this is likely to put different demands on coordination in the IT support function. Under normal operating conditions, coordination efforts in the IT support function would focus on the provision of relevant IT services in a reliable way. However, when emergency conditions arise, service provision is threatened, and the IT function's coordination efforts would focus on *resolving* the emergency in order to *restore* the reliable provision of IT services.

To achieve a deeper understanding of the challenges of coordination in the IT function, we turn to the literature on coordination in organizations.

Coordination in the IT function

Faraj and Xiao (2006: 1157) define coordination as: "a temporally unfolding and contextualized process of input regulation and interaction articulation to realize a collective performance." As Okhuysen and Bechky (2009) argue, "[t]his definition best fits the spirit of [the] recent wave of coordination research, reflecting scholars' shared interest in the emergent nature of the process of coordination" (p. 469). In this study, we analyze how the interdependent work of various individuals in the IT function is coordinated in practice, in order to achieve a "collective performance" in terms of the reliable provision of IT services that meet business requirements.

In studying the coordination of work in the IT function, it is important to realize that this is *knowledge-intensive* work: it requires employees not only to be experts in currently used technologies but also to understand current and future technological trends, as well as the requirements that business places on the IT function (Basselier and Benbasat, 2004). IT personnel are experts who are engaged in knowledge-intensive work to meet the requirements of multiple stakeholders to ensure (continuous) reliability of IS. In this light, the seminal work by Faraj and Xiao (2006) is especially relevant, as it reframes the concept of coordination to accommodate the nature of knowledge-intensive work. They argue that "for environments where knowledge work is interdisciplinary and highly contextualized, the relevant lens is one of practice. Practices emerge from an ongoing stream of activities and are enacted through contextualized actions of individuals" (Faraj and Xiao, 2006: 1157). Adopting the practice lens to study coordination has allowed scholars to enhance our understanding of how complex and highly interdependent work can effectively be coordinated in different knowledge-intensive organizational settings. Hence, our primary interest is in the coordination *practices* found in the IT function, and how these practices play a role in the coordination of the interdependent tasks of different actors with the aim to achieve reliable IT services.

In analyzing these practices, it is important to move beyond traditional coordination theory's focus on studying *how* coordination is accomplished, that is, the mode of coordination. In order to understand the actual practices of coordination, we also need to focus on other dimensions of coordination such as *what* (the content of the interdependent work being coordinated), *when* (the circumstances under which the work takes place), and *who* (the individuals whose actions need to be coordinated in order to realize a collective outcome) (Faraj and Xiao, 2006). First, differences in terminology, meaning, perspectives, and interests impede coordination, creating a need to clarify and agree on *what* the subject of coordination is, and what knowledge is being coordinated. Furthermore, different knowledge boundaries create obstacles for communication between organizational members (Carlile, 2004) which in turn hinder the coordination of work. However, different approaches and specific techniques are required to transfer, translate, or transform knowledge across the different types of knowledge boundaries (Carlile, 2004). Therefore, in terms of *when*, it is important to distinguish between circumstances associated with a specific boundary in order to decide on the appropriate approach to coordinate work across knowledge boundaries. Last but not least, identifying *who* (which specific individuals) are involved in the collective performance, whose knowledge and tasks need to be coordinated, is revealed as an important dimension of coordination, in particular in situations when tacit and personalized expertise is required (Kotlarsky et al., 2014).

As the focus of our study is on how coordination in IT functions changes in response to *emergency* situations, relevant insights can be obtained from recent studies on coordination that pay specific attention to organizations that are often faced with emergencies (e.g. Faraj and Xiao, 2006; Kellogg et al., 2006; Kotlarsky et al., 2014; Schakel et al., 2016; Venters et al., 2014). Examples of such organizations are professionals protecting national security (Jarvenpaa and Majchrzak, 2008), emergency-response teams (Faraj and Xiao, 2006), police work (Schakel et al., 2016), and emergent groups responding to disasters (Majchrzak et al., 2007). In particular, Faraj and Xiao (2006) argue that traditional coordination theory has limited applicability for such *fast-response organizations* (defined as organizations that generally operate under conditions of high uncertainty "where decisions must be made rapidly and where errors can be fatal"; Faraj and Xiao, 2006: 1155) because of the high-velocity environment in which they operate. They argue that

> the dilemma of coordination in such settings is that, on the one hand, there is a need for tight structuring, formal coordination, and hierarchical decision making to ensure a clear division of responsibilities, prompt decision processes, and timely action; but, on the other hand, because of the need for rapid action and the uncertain environment, there is a competing need to rely on flexible structures, on-the-spot decision making, and informal coordination modes. (Faraj and Xiao, 2006: 1557)

This dilemma is reflected in various studies focusing on coordination practices in fast-response settings. For instance, Jarvenpaa and Majchrzak (2008) found that national security professionals tend to prefer their own personal networks over formal organizational structures for the rapid ad hoc knowledge collaboration required in case of an emergency. Similarly, Majchrzak et al. (2007) discussed how emergency situations lead to a shift from formal mechanisms and shared mental models, toward action-based coordination through dialogic practices.[2] Bouty et al. (2012) present a cross-case analysis of coordination in extreme situations which shows a significant heterogeneity of coordination practices in such

Table 1. Key constructs.

Construct	Definition
Coordination process	"A temporally unfolding and contextualized process of input regulation and interaction articulation to realize a collective performance" (Faraj and Xiao, 2006: 1157).
Traditional IT support function	A relatively stable IT support function with a more or less permanent hierarchy, a generally centralized structure, routinized, rule-based and standardized processes, clearly specified and persistent boundaries, and predominantly vertical and dependent relationships (cf. Kellogg et al., 2006).
Fast-response IT support function	An IT support function that generally operates under conditions of high uncertainty "where decisions must be made rapidly and where errors can be fatal" (Faraj and Xiao, 2006: 1155).
Normal operating conditions	"Business-as-usual": operating conditions that an IT support function is prepared and designed for, based on past experience and predictable future changes. Under these operating conditions, we consider an IT function to be in a *normal state*.
Emergency operating conditions	Operating conditions experienced when an IT support function is facing a situation that (1) contains pervasive uncertainty, (2) creates pressure for quick execution, and (3) can have negative consequences such as additional costs or creates a danger of severe physical harm. Under these operating conditions, we consider an IT function to be in an *emergency state*.

situations across the four cases they discuss, finding both highly formalized and vertical, and very informal and horizontal practices based on the specific context of each case.

Although previous studies on coordination in fast-response and traditional settings have been influential in setting the scene for further theory development on coordination, they do not shed much light on how coordination practices *change* in response to disruptions of business-as-usual—what the shift in coordination practices is that accompanies the change from business-as-usual to emergency situations. As illustrated with our examples concerning the IT support function in organizations, IT-related incidents may disrupt these organizations' business-as-usual until they have been addressed in some way. But exactly how coordination of IT support work is adapted in response to such incidents is a currently under-researched subject. This study aims to address this gap, focusing on how the IT function's coordination practices are influenced by the increasing amount and severity of incidents they are faced with. Hence, with this theoretical background in mind (see Table 1 for a summary of key constructs), our empirical research was driven by the question "How does coordination in IT support functions change in response to emergency situations?". Specifically, we ask how the coordination practices of IT support functions in both traditional and fast-response organizations change when operating conditions shift from normal (i.e. business-as-usual) to emergency conditions as a result of IT-related incidents.

In the next section, we explain how we designed our empirical research to address our research question, and the methods we used to collect and analyze the data.

Research design and methods

Research design

Our research was designed as an open-ended inductive study of coordination in a large Governmental IT Service Organization, part of a European country's Ministry of Defense (MoD). This IT Service Organization comprised two IT divisions operating as independent units—one is providing IT services to all civilian facilities of the MoD and the other one is providing IT services to the military (i.e. operational) side of the MoD. As one author was involved in previous research in this organization, we were sufficiently familiar with differences between the two IT functions which we categorized (after careful examination of the literature that distinguishes different organizational forms) as fitting characteristics of a *traditional* and a *fast-response* organization (respectively). Contacts that one of the authors had in this IT Service Organization were used to start a preliminary investigation of operating conditions that both IT functions face and to negotiate access to, and commitment of, the IT Service Organization to this research project. Initial interviews focused on understanding a high-level perspective on coordination in both IT functions. One theme that emerged from these initial interviews was that coordination was accomplished differently, under different circumstances. Intrigued to understand the dynamic nature of coordination in the IT support function we adopted an embedded multiple case design focusing on two units (Langley et al., 2013). To explore changes in the coordination of work, we asked interviewees about their coordination practices when working under normal conditions, about events that triggered emergency conditions, and how coordination of work was accomplished when dealing with an unfolding emergency situation. Our research design and data collection process is illustrated in Appendix A (Figure 4).

Empirical setting

At the time of data collection, the IT Service Organization (hereafter referred as ITSO) had approximately 1900 employees who maintained over 70,000 workstations across the globe, the underlying IT infrastructure and hundreds of software applications. The organization also delivered

additional (IT-related) services such as conducting analyses, giving advice, delivering hardware and software solutions, and developing specific applications. ITSO is the internal IT service provider of the MoD, but also delivers services to other Ministries.

ITSO has two divisions, one responsible for all IT products and services in the civil (non-military) domain—Civit, and one responsible for all IT products and services in the military operations' domain—Milit. As one interviewee explained,

> So if you look at Civit, we mainly manage things in what we call the static domain, anything that's stuck to the ground in our country. As soon as it is mobile, as soon as you go on a mission or an exercise and a network is rolled out there, then it's Milit taking care of it. So that's a different network then—an Adaptive Military Network as we call it—hat can be either "red" or "black" based on the level of confidentiality. But the basic technology is similar anywhere, and those networks communicate with the help of military satellite communication. (Senior Advisor, Civit)

Specifically, as a Process Manager at Civit described what Civit is responsible for on a daily basis:

> We deliver the workplaces all year long and the network and software that runs on it, and all the small standard modifications we will just take care of. Systems management, updates, we make sure it all keeps running, if there are failures we need to ensure that they are resolved, if there are incidents they need to be fixed.

In addition to this ongoing IT support, Civit is responsible for strategic IT planning and implementation of IT-related changes (e.g. replacing all printers with multiplexers that requite to enter one's own code to pick up print).

Milit is responsible for putting in place IT networks and setting up infrastructure to support military missions and armed forces in war zones, including crypto distribution and cyber security management. As the Head of Internal Affairs at Milit described the scope of work that the IT support function in Milit is responsible for:

> Milit has been established for the communication and information systems within the deployment areas and for military exercises. And indeed, some of it is confidential, but also regular message traffic. So here in the office environment [of ITSO] we have a peace network. Just our PC. And in the outlets, they also have the same PC only under operational conditions. So that's actually a very different network, and that's the network provided by Milit. In addition, we [Milit] also use the means of communication, connections, radio connections, satellite connections, so if a ship leaves the port then we also have it, and as a plane flies, the same thing. In addition, we also do the Coast Guard, all ships that go to sea and need to send a signal, and they usually do with HF and that's all the antenna. And therefore we have locations all along the coast line, arming all parts of the coast.

The majority of Milit employees are soldiers in active or previous duty; when required, they travel to provide support in war zones. For example, the Project Office Manager at Milit explained that

> for the people here [at Milit] it is actually normal that if there are problems in the field, during an operation in a deployment area, we will just go there for two or three weeks. Or we'll go there for two months and we'll be back. For the people here, those work visits are no longer called a deployment.

One Civit employee reflected on the role of IT support function and nature of work in Civit and Milit:

> To the extent that the PCs should always work because people have to be able to do their work. And I think if you're working for Defence now or you're working for a retail chain, or if you're working for I don't know who, that shouldn't matter. Not in the work we [IT support function] do. But the moment you really have very specific things like weapon ammunition systems, air traffic control, yes, you have a different situation. (Unit Manager, Civit)

Due to the nature of the military work context of Milit, we can classify this organization as a fast-response IT support function. Milit oftentimes deals with time-critical and complex situations where there is no room for mistakes as, for example, a lack of connection in the operational field may actually cost lives. Civit, on the other hand, is a traditional IT support function. Employees at Civit also deal with emergency situations caused by IS incidents that present different levels of disruption, some of which are serious although (usually) not life-threatening. Both IT functions are physically located throughout the country in diverse military bases and across the globe in former colonies of the European country and in deployment areas. Table 2 describes the differences between the two IT functions along different characteristics.

Background to normal and emergency situations in Civit and Milit

Both IT functions dealt with emergency situations, yet with a different impact on the organization, their employees, and their clients when they talk about normal and emergency conditions. The four examples included in Table 3 describe normal and emergency situations in Civit and Milit in order to illustrate the kind of work that is carried out in each IT function and to provide a general feel of emergency situations.

Data collection

We collected data over a 14-month time period between March 2011 and May 2012. We conducted 33 in-depth semi-structured interviews with employees from all hierarchical layers of both IT divisions and in different functional

Table 2. Background of civilian and military IT functions.

	Civilian IT function (Civit)	Military IT function (Milit)
Type of organization	Traditional	Fast-response
Number of employees	~1700	~200
Nature of the work	Responsible for all IT products and services in the civil (non-military) domain of the MoD	Responsible for all IT for military operations and missions; support Command and Control center of the "defense machine"
Clients	All employees of the MoD and those of the Armed Forces departments working in peace zones; other ministries of the country	All deployed employees/units of the Armed Forces Departments
Percentage of military employees (in active duty or previous duty)	22%	83%
Nature of an "emergency"	Event or situation that presents a (serious) disruption to running "business-as-usual" (e.g. unknown IS incident that is turning into a problem, "important IT unavailable for lots of people," a serious IS incident that becomes a calamity)	Event or situation that requires immediate/ urgent action (e.g. IT for missions, military exercises in preparation for a mission, IS incidents in war zone or active networks, serious IT issues that can cause security breach)
Response to an "emergency"	Resolve to go back to "normal"	Accomplish urgent task in an effective and efficient manner

MoD: Ministry of Defense; IS: Information Systems.

Table 3. Normal and emergency situations in Civit and Milit.

	Normal situation	Emergency situation
Civit	For example, replacing malfunctioning hardware: So when someone's computer is broken and they need a new computer, they report an incident at the service desk. Incident is made, then reported to the Incident Coordinator. They see this is hardware related, have to order new hardware in SAP. A new PC is ordered, then it is reported to planning, a hardware supplier is involved, and a delivery center—and then it is passed on. The logistics center is notified, and the relevant field service engineer, and they are notified that they need to deliver a PC to person X at the delivery location Y. (Senior IT maintenance employee, Civit)	For example, triggered by a serious accident: "A few years back, there was this data center that needs to be cooled otherwise it might overheat and the whole thing crashes. On the roof of this data center there are five air generators of which we need three, or maybe four when it is really hot, to cool the thing and the fifth is a reserve generator, 'in spare'. Then, one breaks down, but well, we still have four left so we can continue cooling anyway. The replacement process takes very long, because it needs to go through a European tender process, because the current service contract has expired. This tender process could take up to a year, so even though that thing is broken, well we still have four left so the priority is low. After a while, the fourth starts to rattle and it also breaks down. At that time, the data center does not receive enough cooling; the temperature starts to rise with all negative consequences following. A crisis evolves and it is this crisis situation that results in a night flight from [another European country] with a mechanic and a new unit in cargo to repair the air generators, where as in the normal process we have been discussing this replacement back and forward for over half a year." (Product group manager, Civit)
Milit	For example, supporting IT for military stations in war zones: "Milit is used to responding to quickly changing situations. For example, during the Afghanistan Mission it was common that in Afghanistan a so-called 'forward operating base' (a FOB), a secured forward military position that is used to support tactical operations, needed repositioning, was dismissed or needed to be replaced. [. . .] New equipment needs to go there, thing must be arranged, configurations require adjustment, and so forth." (Head of Operations Room, Milit)	For example, triggered by IT breakdown during a military mission: "For instance, Afghanistan, those forward operating bases there. When I hear that the connections are gone there, I know what that means. That they can't reach their people. And if they come into contact with opposing forces, that they can't warn their commander. If a call like that comes in from Afghanistan, we know something must be done right away, get things going. So I know at that moment that immediate action must be taken to resolve that. If you get someone who doesn't have that military past, or is not really part of the military organization, he won't see that. He will think 'so he can't call, who cares that two units can't contact each other for a while?' You notice that if people don't have that military past, it's harder to get that understanding." (Head of Knowledge Pool, Milit)

roles (see details of the interviewees in Appendix C, Table 9). Participants were motivated by ITSO to contribute to the study as the commanding officers from Civit and Milit wanted to address coordination and knowledge sharing practices in both IT divisions of ITSO. Almost all interviews were taped and transcribed verbatim. Interviews lasted from 45 min to over 2 h in length and were conducted on a one-on-one basis, except for two interviews that involved two interviewees at the same time. One author also spent time talking to employees informally, joining them for lunches during her visits to different military bases. She also participated in several management team meetings as an observer. In addition to the interviews and observations, we also gained insight into the formal meeting structure at both IT functions and documents describing projects (e.g. project initiation documents), work instructions (extended documents containing examples for several functional roles), and process guidelines. This secondary data provided important contextual information about both IT functions of ITSO.

As we intended to distinguish between coordination practices during normal and emergency states, we started the interviews by establishing a clear understanding of the difference between *normal* and *emergency* operating conditions, as perceived by the respondent's IT function. We then proceeded with open-ended questions to explore coordination activities and practices in which the interviewee was involved in his or her daily work under normal conditions. We asked about events that triggered changes to emergency conditions and how coordination was accomplished when dealing with the emergency situation. We used the four dimensions of coordination recognized as important for understanding coordination processes in knowledge-intensive settings—*what* (content), *how* (mode), *when* (circumstances), and *who* (which specific individual is the person to contribute to joint coordinative efforts)—as a checklist to ask for clarifications and further details as interviewees were describing activities and practices (s)he was involved in to coordinate IT work. For example, if an interviewee was describing *how* (s)he was solving a specific IS incident, we would ask *who* were people (s)he was contacting. (Our data collection process is illustrated in Appendix A, Figure 4.)

Data analysis

Given the inductive nature of this research aiming to understand the dynamics of coordination in IT support functions as they face emergency conditions, we followed guidance provided in Langley et al. (2013) for theory-building about change, as well as Langley (1999) for specific data analysis techniques. Specifically, we used a temporal bracketing strategy in our analysis to distinguish between periods when (1) coordination took place under normal conditions, (2) coordination took place under emergency conditions, and (3) the shift from normal conditions to emergency conditions. These periods are described as Episodes 1, 2, and 3 (respectively) in the "Analysis" section.

Interviews were transcribed and coded using NVivo qualitative data analysis software. Data analysis followed several steps. It relied on iterative reading of the data using the open-coding technique during which first order or subject codes were assigned (Gioia et al., 2013; Strauss and Corbin, 1998). Through sorting and refining themes emerging from the data, we applied the axial coding technique (Miles and Huberman, 1994). In accordance with our embedded multiple case design, as we were moving from first-order concepts to second-order themes, we first distinguished between the two cases (Civit and Milit) and analyzed them separately (in steps 1–3) before moving to cross-case analysis (step 4). Our data analysis process is illustrated in Appendix B (Figure 5).

Step 1: analyzing events that triggered change in coordination

We coded and analyzed events that triggered changes in operating conditions. As each interviewee was asked about events that disrupted "business-as-usual," and how they affected coordination, this allowed us to explore the nature of the shift from normal to emergency conditions based on replication of temporal observation (Langley et al., 2013) of such shifts triggered by the events.[3] This analysis led us to distinguish between different natures of "emergency" in Civit and Milit (as illustrated in Table 2) and used for further analysis of the shift (as described in step 3).

Step 2: analyzing coordination under different operating conditions (within-case analysis)

We coded and analyzed activities associated with coordination in Civit and Milit, making a distinction between activities that took place under normal and emergency conditions. Through iterative sorting of activities into themes and refining of emerging themes, we arrived at four second-order themes that distinguish between four coordination practices: *prioritizing tasks, following procedures, using roles and responsibilities*, and *utilizing networks*. We continued our analysis and moved on to map inter-relationships between these practices: *defining, prescribing, following*, and *deciding* (as we discuss in the summaries at the end of Episodes 1 and 2). These inter-relationships are illustrated in Figures 1 and 2 using arrows that show how one practice influences or triggers (an)other practice(s), and what the nature of this influence/trigger is.

Step 3: analyzing how coordination practices were "adjusted" when faced with an emergency (within-case analysis)

Based on the data coded during step 1, and an understanding of how coordination was accomplished under normal and emergency conditions (based on step 2), we could focus our analysis on the shift from a normal to an

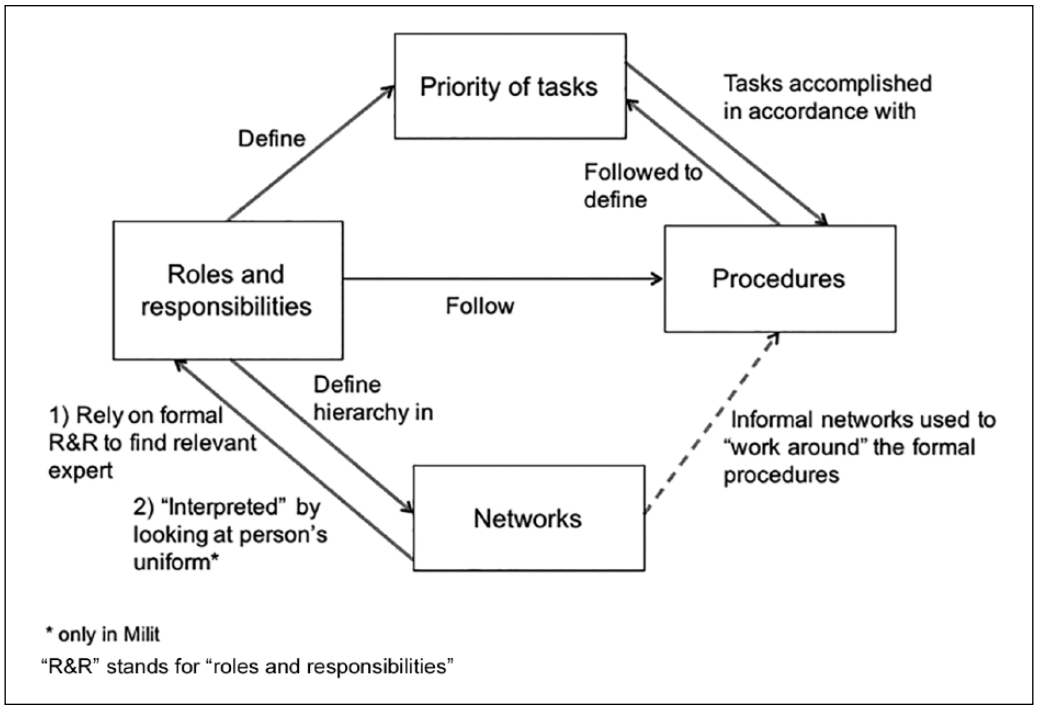

Figure 1. The dynamics of coordination under normal conditions.

emergency state, aiming to conceptualize characteristics of the shift, including the time-dimension. We distinguished different events that triggered the shift. Categories of these events and exemplar quotes are included in Tables 6 and 7. Second-order themes that emerged distinguished the nature of the shift in the two IT functions as chaotic (in Civit), and formal and well-structured (in Milit). Our analysis of the shifts is presented in Episode 3 in the "Analysis" section.

Step 4: analyzing dynamics of the coordination process (cross-case analysis) toward theorizing

This step focused on iterative analysis and refining of our conceptualization of the shift and coordination under emergency conditions in Civit and Milit (as illustrated by loops 1 and 2 in Appendix B, Figure 5). Furthermore, we analyzed how inter-relationships between coordination practices (conceptualized in step 2) change when IT functions shift to a state of emergency (i.e. how change in one practice triggers change in another practice). We compared the observed patterns of changes between Civit and Milit (a change from the inter-relationships depicted in Figure 1 to the inter-relationships depicted in Figure 2—top square for Civit and bottom square for Milit). For example, the coordination practice "using roles and responsibilities" *defines* "prioritizing tasks" in all circumstances except when Civit is facing an emergency (top square of Figure 2). In such situations the "prioritizing tasks" practice is triggered by an IS incident or calamity, influencing the "using roles and responsibilities" practice that invokes actions from escalation and crisis managers who are expected to facilitate resolution of the emergency situation.

This step concluded our data analysis and provided the basis for "climb[ing] the ladder of abstraction by inferring the general theoretical phenomenon of which the observed particular is a part" (Langley et al., 2013: 8) toward building a dynamic view of coordination process in traditional and fast-response IT support functions.

Analysis

Based on our analysis aiming to understand how the Civit and Milit IT functions coordinate work and how they change their approach to coordination when faced with emergencies we identified four high-level coordination practices enacted in these IT support functions: (1) *prioritizing tasks* is establishing *what* will be coordinated and *when* this coordination is to take place; (2) *following procedures* is capturing formal ways to determine *what* should be coordinated and *how* this should be done; (3) *using roles and responsibilities* indicates *who* should be responsible for coordinating *what* (or *who* is likely to be an expert in *what*); and (4) *utilizing networks* depicts formal and informal links between individuals that explain *who* coordinates *what* and *how* it is achieved. Our findings indicate that these four practices may be enacted in various ways, that is, through a repertoire of different coordinative activities (as demonstrated in Tables 4 and 5). While Civit and Milit coordinate work in a similar manner under normal conditions, these two IT functions respond differently to an emergency. In

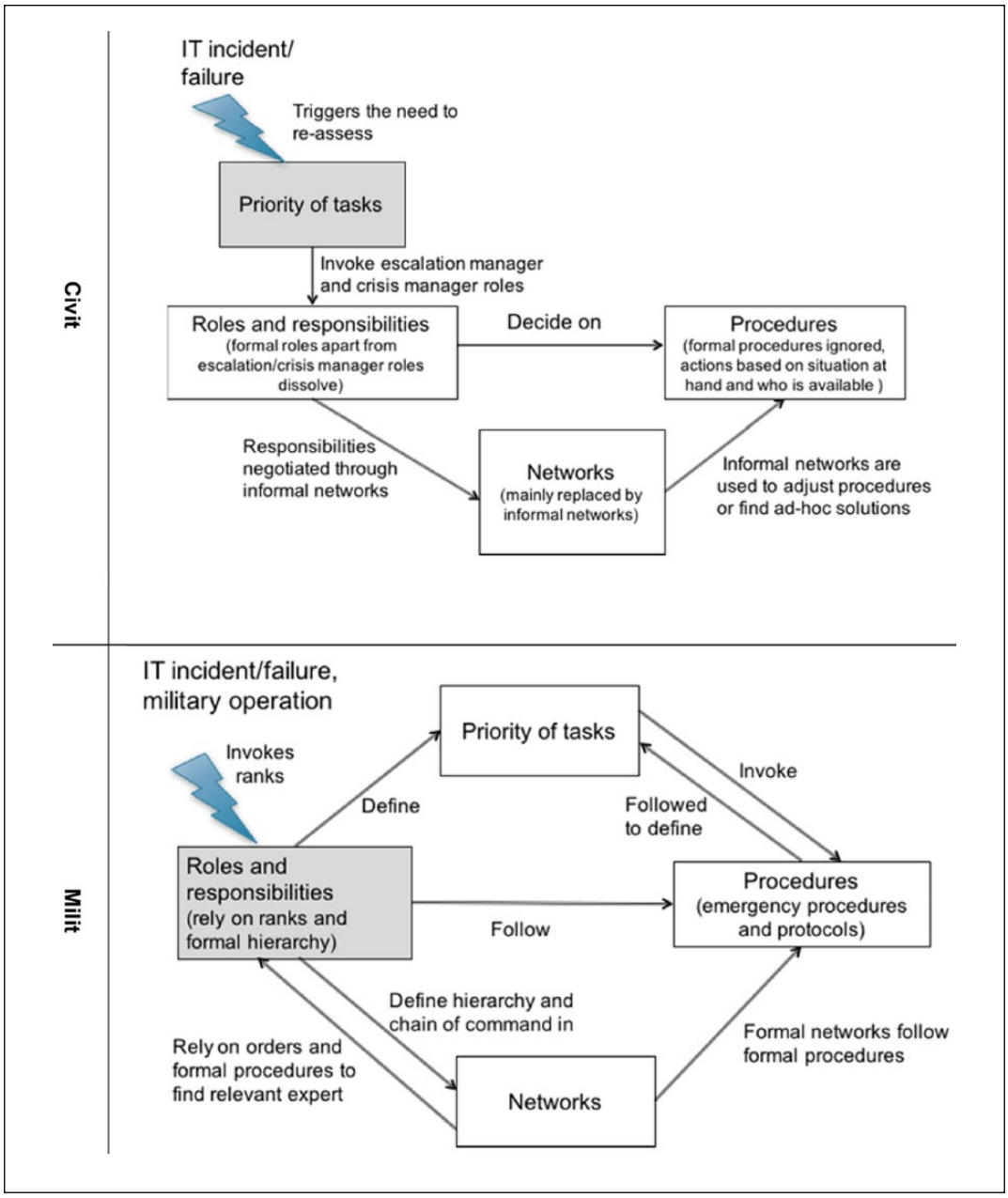

Figure 2. The dynamics of coordination under emergency conditions.

both cases, the enactment of coordination practices changed in response to emergencies, but the actual changes are quite different when we compare Civit and Milit. To illustrate this, we present our analysis of coordination in the two IT functions (Civit and Milit) focusing on three consecutive episodes. We will first discuss coordination under normal operating conditions. Then, we will discuss how coordination had changed after IT-related incidents that created emergency conditions. Subsequently, we present our analysis of the period of time associated with the change: the shift in coordination practices as a result of an event that disrupts "business-as-usual." As we demonstrate, while four coordination practices are evident under both normal and emergency conditions, the inter-relationships between these practices change when IT functions face emergency conditions.

Episode 1: coordination under normal conditions

Under normal conditions, Civit's main *priority* is maintaining 70,000 workstations and a multitude of IT systems. Incoming IT-related requests from clients (which can be internal within Civit, external within the MoD, or external

Table 4. Coordination practices and comprising activities under normal conditions.

Coordination practices	Activities comprising coordination practices	
	Civit IT function	Milit IT function
Prioritizing tasks (what and when)	Using formal meetings to negotiate or impose priorities of tasks Using Standard Requests, Non-Standard Requests, and Projects Using service-level agreements (SLAs) to set standards in solving problems	Using formal meetings and "morning prayers" to prioritize tasks Using Standard Requests, Non-Standard Requests, and Projects Using SLAs to set standards in solving problems for clients
Following procedures (what and how)	Following formal procedures and processes Through ITIL, PRINCE, and SLAs	Relying on formal procedures, especially those concerned with confidential processes Through ITIL, PRINCE, and SLAs
Using roles and responsibilities (what and who)	Relying on a person's functional (formal) role (RACI matrix) Using digital directories/databases to find relevant person according to their role/responsibility Assigning tasks according to experience Through meetings responsibilities are assigned to people	Relying on visual indicators such as person's uniform which indicates background, experience, and rank to "interpret" their role/responsibility Relying on person's functional (formal) role Using digital directories, for example, functional e-mail boxes Assigning tasks according to experience with a specific client Using "Morning prayers" to discuss and assign responsibilities
Utilizing networks (what, how, and who)	Following the formal and hierarchical lines Using informal networks to "work around" the formal organization	Using formal networks that are associated with formal procedures Using informal networks built through shared or similar experiences, assuring trust

ITIL: Information Technology Infrastructure Library; PRINCE: projects in controlled environments.
The RACI matrix captures four key dimensions of involvement with a task: Responsible, Accountable, Consulted, and Informed.

Table 5. Coordination practices and comprising activities under emergency conditions.

Coordination practices	Activities comprising coordination practices	
	Civit IT function	Milit IT function
Prioritizing tasks (what and when)	(Always) putting incidents and calamities first (no time to negotiate other priorities of tasks) (Sometimes) exercising power to accelerate action: "the one who shouts the loudest" Systems are used to register incidents, but do not prioritize them	Relying on formal mechanisms; putting incidents and accidents first Conforming to highest in command who decides (but also consults with the experts)
Following procedures (what and how)	Using "carte blanche" (crisis mandate) to act own's discretion to remove steps, "ignore" procedures Looking for informal ways to resolve the situation (work around the formal line)	Relying on a very formal approach: plan-do-check-act Relying on formal structures and protocols Having zero tolerance for mistakes (attitude)
Using roles and responsibilities (what and who)	Institutionalizing crisis "functions": crisis managers and escalation managers Acting based on situation at hand and "who is available" (no time to formally assign responsibilities) Using "carte blanche" to assigning people to a certain task	Following "command and control" which relies on exercising power based on rank and role and obeying orders (uniformity) Responsibilities are associated with the uniform, the higher the rank, the more responsibilities Using digital directories such as functional e-mail boxes to assure direct response (staffed 24/7)
Utilizing networks (what, how, and who)	(Mainly) using informal networks to retrieve relevant knowledge as people do not have time to verify expertise or build trust Reliance on "people we know and trust"	"Enforcing" utilization of formal networks only Building trust through reliance on uniforms, rank, and formal military procedures

organizations) can be standard (e.g. setting up a new workstation for a new employee), non-standard (e.g. request for a new custom-made application), or a specific project. For standard and non-standard requests, there are set rules and regulations regarding the time to deliver the requested need, based on the impact of the problem for the user of the system, giving clear guidelines on what steps or procedures to follow to fulfill the request. Priorities are discussed

during formal work meetings and tasks are carried out according to the set times. The Head of the Cluster Security & Identity at Civit elaborated about priorities for projects, and the impact on possible IS incidents:

> Projects can also have a lot of priority and then you might have to get people to work late, put in extra hours. So if we do not comply with our current contracts, we decide that it's better for the ministry so that 10,000 people cannot work because their account is not operational, for instance? So we need to consider priorities, of course. Our colleagues at Processes make those considerations, but I do not know if I always agree with the priorities they make. I think they are cutting back too much on regular maintenance, with the result that we will have more incidents and calamities in the future.

Milit employees often deal with similar requests as their Civit colleagues, but work within Milit usually concerns military-operation systems and clients who work in active military missions or training areas. For example,

> If people, embassy employees for instance, get the equipment and stuff, they get it at the airport or at home, they get it and then they can take it with them. All missions, deployment missions, start with that. That's all starting there. There we need to set up whole structures to ensure that everything that goes with crypto goes well. (Head of Information Security, Milit)

The way Milit employees deal with incoming requests is somewhat different from Civit (as evident from the list of activities included in Table 4). For example, Milit has so-called *morning prayers* at several locations, where every morning at 7:45 AM, tasks and projects are discussed and priorities are set for both the short and long(-er) term.

Procedures play an important role in coordinating IT work and finding expertise required to execute different tasks. In Civit, employees are expected to follow formal procedures at all times. Procedures are institutionalized through ITIL (Information Technology Infrastructure Library; a set of practices for IT service management that focuses on aligning IT services with the business), PRINCE (projects in controlled environments; a project management methodology), as well as through securing deliveries to clients via SLAs.

Because of the nature of the military work, Milit has a zero-tolerance policy for mistakes regarding many procedures. When it comes to classified projects or services, every step of the process must be followed "to the letter." Access to secure networks and authorizations are among aspects that follow specific approval procedures. On the other hand, there are situations when Milit employees deviate from formal SLAs in order to solve an urgent IS issue, based on experience of the people involved and their assessment of the situation. This is illustrated in the following example of a situation when Milit received a non-standard (and complex) request that needed to be dealt with quickly and properly. This request came in at the operations room [the bridge] right before the millennium night of 30 December 1999:

> We discussed, weeks ahead of time, the controlled shutdown of the mainframe with our clients. We would shut down the systems and the applications at 22:00 and bring them back up at 2:00. Based on the letter we sent out to the helicopter group at D [City], which was back then still part of the Navy, I received a phone call from the colonel "we need to provide support and when the system is down, we can't access our stock lists." They need to know exactly what they have in stock, because equipment is certified and otherwise helicopters cannot fly. I proposed to download their information, burn it on a CD and send out a courier to them with stock information at 21:00 to consult during this night.

To coordinate IT work, members of Civit and Milit rely on knowledge about who-knows-what which they develop in a variety of ways, for instance through perceptions of relative expertise of others which are usually associated with *formal roles and responsibilities*, or through stereotyping. In Civit, assignment of roles and responsibilities is formalized through a hierarchical role index where a role is a descriptor of an associated set of tasks that can be performed by many people and one person can perform many roles. This IT function relies on formalized procedures describing the person (the role) to contact for different issues or requests (e.g. if an employee is requesting a new desktop or application, the procedure would describe whom to contact and what form to fill in). Under normal circumstances, the assignment of a person to a task is based on their formal role and function and is matched with their expertise. Experience of the employee with the type of project, or the client, also plays an important role. Within several sub-functions of Civit, initiatives were put forward to capture all employees' expertise, skills, and experiences with clients in a system combined with educational information in order to facilitate the search for information.

In Milit, employees are recognizable according to their uniform, indicating from which Armed Forces Division (Navy, Army, or Air Force) they stem, and their "stars and stripes" indicate their rank. The uniform provides a good indication of a person's background and experience, both in terms of the client information (as the uniform corresponds to the Armed Forces Division, which are all clients of the Milit) and years of experience within the Defense organization (rank approximately indicates tenure in the Armed Forces), but not necessarily their specific role in the IT function (Milit). Under normal circumstances, Milit employees rely on formal roles that are associated with specific functions. Allocation of tasks can be both person-based and expertise-based. In particular, when specific expertise is needed to address a high-priority issue, a fast response is expected when sending out an email with a

request for information to a functional email box instead of approaching a specific person. For example, as one Senior Project Manager at Milit explained,

> In military departments, you almost always have functional e-mail boxes. You send a request for information not to someone, but to the e-mail box. So you don't send an email to just one specialist, behind this e-mail box are usually several specialists and always one will answer immediately. This is the military principle.

In Milit, the most important aspect when assigning responsibilities to an employee is experience with a client (i.e. specific Armed Forces). It appears that this client-specific experience prevails over project- or task-domain specific experience within Milit. For instance, when two employees with similar product-domain knowledge (e.g. about a specific IT system) or project-domain knowledge (e.g. establishing connections with a mission area) are available, the one who has more client-specific experience is assigned to the job.

To coordinate work, employees in both IT functions rely extensively on *networks*. Within Civit, finding relevant expert relies primarily on formal networks. Civit institutionalized a very formal system through which every step is monitored or "otherwise we lose control" (Process manager at Civit). At the same time, informal networks are also very important in Civit. As individuals work together on joint projects, they get to know one another and their areas of expertise, and they use this knowledge at a later stage to contact their peers when relevant expertise is required. Through such shared experiences, informal networks emerge. Indeed, some people are very active in forming informal networks across the IT function:

> When I look at my own function [product group manager], I "network my ass off" to get the best possible informal and "like knows like" network. That also means I actively contribute to these networks. Anyone can call me at any time with questions such as "I have a problem; can you help me with this and that?," "How would you do this?" (Product group manager at Civit)

In Civit, informal networks are used to get things done more quickly, while avoiding the formal hierarchy embedded in the organizational structure and creating shortcuts. For example, one can send an informal message first notifying the receiver that a formal request will follow. However, this is *only* done when people know each other. This function seems to be "stuck in its own formal process, that's why we have a massive informal circuit" (Delivery manager at Civit).

In Milit both formal and informal networks are utilized by employees to find relevant expertise. In addition to networks that are built through shared collaborative experiences, Milit employees often share similar experiences which are accumulated separately by having been at the same place or situation, rather than by active collaboration or shared past experiences, such as having followed the same military training, or having participated in the same military mission. Such common experiences are evoked by recognizing the same uniform or rank; there is an implication of trust and, to some extent, a perception of a similar expertise. These common experiences are used in informal as well as formal networks. Informal networks can be very useful in preparation for military operations, as illustrated in this example:

> On Saturday, the Arab League called upon the UN Security Council to impose a no-fly zone on Libya. During the UN Security Council meeting on Tuesday, Lebanon tabled a resolution for a no-fly zone to be imposed over Libya. Actually, one day earlier, on Monday, the [informal] call came in at Milit that the European Country's Air Forces probably would support the enforcement of this resolution. They [Milit] had already started with the preparation of IT necessities for fighter jets, even though there was no formal assignment yet. I was happy we'd already started with the preparations, because on Thursday, the formal assignment did come in and that same weekend we already had to send gear in that direction. Had we not started on Monday, we would never have made it on time. (Head of Knowledge Pool at Milit)

Summarizing inter-relationships between coordination practices in Episode 1. Under normal operating conditions, *priorities of tasks* are defined by those having formal roles to do so, and those priorities are accomplished in accordance with the *procedures* at hand. At the same time, following these procedures *defines the priority* of (other but related) tasks. Formal roles that are captured in the organizational structures of the IT functions (Civit and Milit) *define hierarchy* which is followed when coordinating via formal networks. Consequently, individuals *rely on formal roles and associated responsibilities* to find colleagues with relevant expertise. Informal networks are used occasionally to "work around" the formal procedures to speed things up. Figure 1 depicts the dynamics of coordination in both IT functions under normal conditions.

There is, however, one difference between the two IT functions in terms of the way the roles and responsibilities are relied on and interpreted through the networks. Milit employees are often able to "interpret" what experience and responsibilities their colleagues have by looking at their uniform, which shows the Armed Forces Division (e.g. Navy or Air Force) and their rank. A uniform, however, does not give any indication of a person's specific level of expertise or knowledge related to IT services. In that regard, civilian and military employees are in the same position, utilizing inter-personal relationships and awareness about specific expertise of their colleagues, when relying on informal networks to coordinate work faster. Based on this analysis, Table 4 provides an overview of activities

that constitute coordination practices in the two IT functions under normal conditions.

In the next episode, we discuss in detail how Civit and Milit coordinate work under emergency conditions.

Episode 2: coordination under emergency conditions

When Civit employees are dealing with an emergency situation, they need to address the issue quickly to avoid further disaster. Therefore, tasks associated with resolving the emergency situation become the first *priority*. For example, when a whole system shuts down and thousands of employees are without a network connection, priorities on standard and non-standard requests and projects are put aside and the situation at hand becomes the focus of all activities. Thus, coordination efforts are focused on finding experts that could help to resolve the emergency situation. What sometimes happens within Civit is that, due to time pressure and busy schedules, during formal meetings some priorities are misaligned with reality or overlooked. As one of the product managers at Civit noted,

> No one sets priorities, everybody keeps shouting, emailing, and calling and, in the end, no decisions are made. Some tasks are ignored under pressure, like extensive maintenance of systems. You can compare this with your car: if it needs a check-up, it does not need to be done right now, you can also do it next week. With IT networks we see the same thing: it does not need to be done right now, we can do it next week. If you do this one too many times and you postpone half a year with your check-up at the garage, you'll find yourself one morning with a low battery, your car won't start. It is therefore of the utmost importance to set priorities and control this process.

What happens is that certain tasks remain "on the shelf" until they become the source of an incident. Then they receive a red flag, become a calamity, and suddenly rise to the top of the to-do list of Civit. As a Process manager at Civit commented, "We have elevated crises, even if they aren't, we are crisis-oriented to get things done around here." Indeed, as a Unit Manager in Civit explained, creating (sometimes artificially) an incident or calamity is the way to speed up things:

> I've also talked with a lot of people and what I hear very much within I & S is that it's very formal and it's very bureaucratic and it's slow, it's very slow. What it actually means that it's very difficult to match priorities for standard and non-standard projects. So, when something really has to be done, it's easier or more effective to make it an incident or a calamity, because then people will start running. So what that means is, we call "fire" earlier than we used to, because then it works. Yes, in practice it often works that way. The only thing is, I think very often that a calamity or incident is created or called, without it being real. So at a certain moment, there's this feeling of "oh, it's probably not so bad"—you get used to it. So then, every time it needs to be presented as more serious, and there's an upper limit to that as well. So yes, we have an escalation manager, and that's not necessarily a bad thing, but why do we have an escalation manager?—because in the hierarchical line, in the regular organization, people just don't succeed in coordinating things properly, taking responsibility, making decisions. That's why we now have an escalation manager, and that's where we need to bring those incidents.

In Milit, in a state of emergency, tasks associated with the emergency situation must be carried out immediately, putting ongoing tasks and projects on hold. *Prioritizing tasks* in Milit is driven by the importance or severity of a situation associated with a specific client. Milit internally refers to this as a "client-based perspective." For example, one router that is malfunctioning leaving only one agent in the military activity zone without a connection may be much more important than a malfunctioning router that serves 50 individuals on the safe base. As the Head of Operations Room at Milit explained,

> You should not assess the situation based on whether this is one workstation that does not work, or here we have 20 workstations that do not work. No, you should keep the client perspective in mind and assess the importance of the situation and when that single workstation is more important than those other 20, then those 20 will just have to wait a little while. If you look at it from an IT network perspective, and you have never been on a mission and don't know the backgrounds, you only see 20 people without a connection and you think that needs to be solved first.

In contrast to Civit, where prioritization in emergency situations becomes an issue, in Milit the highest in rank usually decides what to do, and instructs the others down the pyramid accordingly. However, decision-makers do listen to the experts when it comes to dealing with certain situations; thus if possible, the decision is agreed on by, or verified with, the expert on the topic.

In Civit, when dealing with an emergency situation, "formal procedures are put overboard" (as one interviewee put it); as in the earlier emergency example where a new cooler for a data center was flown in within a day, while the actual replacement procedure was to go through a long tender process. In Civit, there is a sort of "carte blanche" (i.e. unrestricted power to act at one's own discretion, also referred to as a crisis mandate) in crisis situations, which means that "we don't have to go through 16 steps before reaching an approval state" (Senior project manager at Civit). This means that formal procedures of Civit that are designed for dealing with "normal" IT requests and incidents break down in emergency situations when urgent action is required. However, there are no emergency procedures to kick in under such circumstances. Therefore, formal procedures are replaced by shorter, much more informal ad hoc actions aimed at resolving the incident by any means possible.

Different from Civit's approach to coordination under emergencies, Milit follows the military way of doing things under emergency conditions as illustrated by a Senior program manager at Milit: "Under emergency circumstances it's important to go through the plan-do-check-act phases as quickly as possible, in order to stay ahead of your opponent." In emergency situations, military employees greatly rely on formal structures and protocols. So where, in Civit, the plan-do-check-act cycle is being reduced by removing steps, people and parts from the normal procedures, in Milit the principle is to follow the *procedures* (even more) "to the letter," only much quicker. Hence, coordinating work to resolve emergency situations and address urgent IT requests is a highly formalized and efficient process within Milit. Specifically, the way in which Milit personnel use these formal procedures is closely linked to the formalization of roles and networks that are utilized.

Civit, being a large IT function with many hierarchical layers, formalized a number of crisis *roles* such as "crisis manager" and "escalation manager," which have been institutionalized to deal with emergency/crisis situations. These crisis roles come on the top of other (normal) responsibilities that these (usually higher-/management-level) individuals deal with on a daily basis. The person in this role is the first to be contacted in case of an emergency and s/he becomes the main contact point until emergency is resolved. As one interviewee elaborated,

> We got these escalation managers because we saw that people down the line were not well connected and did not take, or did not dare to take on responsibilities. So now we have a "location" to bring our trouble to. However, this actually does not resolve anything, because these people also have to fine-tune decisions "along the line." (Unit manager at Civit)

One escalation manager described his role as: "I am a hub, connecting people, building bridges, connecting people, resolving issues." He explained that he knows that he cannot act under time pressure in situations that are too complex, but he is active in managing part of the complexity of situations within the organization. Some of these crisis managers are the only ones who can "wake up" the entire organization in case of an emergency.

As the crisis mandate effectuates, there is a "carte blanche" when it comes to assigning people to a certain task, if they are considered to have relevant knowledge to get things done. In an emergency, formal rules and procedures do not apply anymore, as action needs to be taken immediately—otherwise the impact of the incident or calamity can be disastrous. The need to avoid a disaster may foster collaboration between individuals who join their efforts in trying to address one common goal. For example, as a product group manager at Civit explained,

> What happens is that all of a sudden there is room for cooperation, sharing knowledge and coming to a joint solution, where before everyone was only looking at their own piece of responsibility.

When Milit is dealing with an emergency situation, the reliance on roles and responsibilities within this IT function shifts from a formal cooperation mode to "hierarchy and command." As one of the interviewees illustrated,

> First your name is just Ralph, and I am Captain Brian. Suddenly things do not work anymore and then the boss says "Lieutenant Stacey." It is at that moment when he calls you by your rank and last name, that he invokes his rank and you have sworn to blindly follow a higher rank. (Senior technical specialist at Milit)

There is a clear formalization in case of an emergency. The example given under normal circumstances about the functional e-mail boxes also applies here; Milit has institutionalized several mechanisms to assure a direct response when faced with an emergency. Milit is a 24/7 organization, employees are trained for and used to this context and rely on their formal roles to deal with emergencies.

When employees in Civit feel that a certain situation escalates to a state of emergency, they seem to rely mainly on their personal informal *networks* to quickly access relevant knowledge. Since emergencies require rapid action and there is no time to verify expertise and get approvals through the formal procedures, people can only go to those colleagues they know and trust as an expert in a particular area. Considering the crisis mandate explained earlier, the formal procedures are avoided in order to get access to the right expertise quickly. Therefore, informal networks are key when coordinating during emergency situations in Civit.

In Milit, according to the military principle (captured in the Code of Conduct to which military employees swear to obey), obeying orders and following procedures are key when dealing with emergency situations. In accordance with this principle, the formalized way of coordinating work is evident in Milit during the emergency state. Employees follow strict instructions in complex situations and do not deviate from the formal line of command. In contrast to Civit where formal networks are replaced by informal ones under emergency situations, in Milit formal *networks* become even stricter as staff purely rely on ranks and the hierarchical chain of command. Ranks and military protocols define who is in charge in emergency situations and who is following whose command. Who-knows-whom and inter-personal relationships are abandoned and only orders and protocols invoked through the formal chain of command are followed.

Summarizing inter-relationships between coordination practices in Episode 2. Under emergency operating conditions, the dynamics between coordination practices unfold differently in Civit and Milit (see Figure 2). Triggered by a

serious IS incident, in the traditional IT function (Civit), the priority of tasks changes so that all coordination efforts are focused on dealing with the incident that has caused the emergency. Avoiding further disaster and returning to business-as-usual becomes the main priority. This priority, in turn, *invokes different roles* (such as escalation and crisis manager) that mobilize individuals affected by the emergency, and these individuals attempt to resolve the emergency by coordinating in an ad hoc, improvised manner, heavily *relying on* informal networks, *ignoring or adjusting* formal procedures and deciding on which procedures (not) to follow. In contrast, in the fast-response IT function (Milit), an event that triggers an emergency situation *invokes* formal and hierarchical roles based on military ranks that, in turn, switch to coordination based on emergency protocols, and obeying orders based on a command and control framework. Ranks and accompanying responsibilities are never questioned. The higher in command *defines* the priority of tasks which, in turn, *invoke* relevant emergency protocols and procedures. The coordination efforts are concentrated on *following* emergency procedures. Military rank *defines* the chain of command in formal networks. Then orders and emergency procedures are followed to find relevant experts and coordinate their actions. Thus, the way Milit accomplishes its mission in an emergency situation is through its military doctrine which prescribes order, uniformity, and control on all operational levels with a zero-tolerance to any forms of misconduct or deviations from formal procedures. Deviation from the command and control framework could potentially lead to disaster (Farrell et al., 2013). These inter-dependencies between coordination practices are captured in Figure 2, which illustrates how coordination unfolds under emergency operating conditions in Civit and Milit.

Derived from the analysis presented above, Table 5 provides an overview of activities that constitute coordination practices in the two IT functions under emergency conditions.

In the next episode, we focus on the *change* in coordination practices when IT functions face emergency conditions. We conceptualize this change as a "shift."

Episode 3: the shift—responding to an event until "emergency" state is established

This episode is describing a period of time which is substantially shorter than those depicted in episodes 1 and 2 where we discuss how the coordination process unfolds under normal and emergency conditions. However, it is crucial to understand how the shift in coordination occurs in traditional and fast-response IT support functions (Civit and Milit, respectively), that is, what happens after normal operating conditions are disrupted until an emergency state is declared. Our analysis of events that disrupt the normal state illustrates that in Milit there is a clear vision of what constitutes an "emergency" and therefore requires urgent action. Such events include IT issues/incidents during a military operation (in a war zone); projects requesting to provide IT support in preparation for a mission; urgent IT problems that happen during a mission or exercise; IS incidents or problems in what is referred to as "active networks" (i.e. in the field); serious IT issues that can cause a security breach; and life-threatening situations that can become an emergency if not addressed as a matter of urgency. These events (illustrated by exemplar quotes in Table 6) *trigger* enactment of the emergency state, which happens momentarily.

In Civit, there is no such clear shift from a normal to an emergency state. Events that disrupt business-as-usual in Civit are not considered immediately as emergencies but rather escalate or lead to further disruptions until they become a "crisis situation" or "calamity." Thus, different from Milit where certain events *trigger* the shift to a state of emergency, in Civit events typically *lead to* a state of emergency over time. Such events include unknown IS incidents that turn into a problem; systems being down (i.e. "important IT unavailable for lots of people"); a serious incident that causes systems breakdown and becomes a calamity; IT failures that become high-priority issues; IS incidents that escalate; IT requests that are escalated because they cannot be accomplished in time according to SLAs; and high-priority assignments due to resourcing constraints. Categories of these events are illustrated in Table 7 and illustrated by exemplary quotes.

An event that disrupts the normal state invokes changes in coordination practices, and the way these changes take shape differ substantially between the two IT functions. When an incident disrupts the normal functioning of Civit, this is manifested in a breakdown in "normal" coordination practices. It takes some time for Civit to establish the extent of an emergency (e.g. how many and which clients of the IT function are affected and whether the situation is still unfolding and could lead to further disaster) and to adjust existing coordination mechanisms (or put in place new ones) that would resolve the situation so that Civit can go back to "business-as-usual." The earlier example (in Table 3) of a severe accident when two air generators of the data center broke down portrays a situation when unfolding events (breakdown of one air generator after another) made this incident evolve into an emergency as the second air generator stopped working. It took time for Civit to realize the severity of the evolving situation and to establish that following the formal procedure (tender process) would not allow resolving the situation. They acknowledged the state of emergency and started looking for ways to repair or replace the generator(s). At the end, an expert was flown from another European country, as well as a new air generator.

When Milit is facing an event that is considered as a trigger for a shift to an emergency state, Milit acts quickly. In such situations, whether it was planned in advance (e.g. a military operation) or happened unexpectedly (e.g. a sudden IT breakdown), lives of soldiers deployed are at stake,

Table 6. Categories of events that *trigger* emergency state in fast-response IT support function (Milit).

Category of events that *trigger* emergency state	Exemplar quote
IT issue/incident during military operation (in a war zone)	The commander in Afghanistan says "Hey man, I cannot connect with my units in the field." But OK, that man really is out there—while I'm behind a desk but they are really out in the field walking around with a gun. So if a Commander in Afghanistan says that he can not get connected through a classified connection because a particular device is no longer working, then it has to be picked up immediately. You can not let that be bogged down by some bureaucratic red tape—this goes straight from Afghanistan to the ministry and 2 seconds later I'm right on it. ----- If it is already clear that there something going on with crypto {i.e., cyber-security issue with crypto service], then the Operations Room will let go of it immediately and say that they need to go to me. Or actually to the ministry, there's someone who coordinates all that—and that's all coming to me, and that's yes. That has to be done right away, immediately. --- If a call comes from Afghanistan saying "we have this problem," something needs to be done. If it does not go through a formal line, then you can get things done immediately via an informal line. You notice that if you do not have that military past it's harder to get an understanding of that. This also has to do with simple things as abbreviations. If you spend longer time in the defense organization, at one point, of course, you understand those things. --- Example of IT breakdown during a military mission in Afghanistan—see quote included in Table 3.
Project to provide IT support in preparation for a mission	*Interviewee*: Yes, there is a capacity limit. *Our question*: But what happens if there is a request for a new project to support a new mission? What if you don't have the capacity to manage that project? *Interviewee*: If it is a mission, then it means that a political decision has already been taken, then it has to go on. Then an operational compartment must be released. That usually means that when there is an exercise, that exercise stops. Then the capacity moves to the mission. The Libya mission had that. Only then we used another trick. We have added that to the operational compartment of our Afghanistan mission. That was accepted by the staff in Location B. Formally, that is not entirely correct. But if they say "we buy it" then we'll do that. We do that for exercises, for example. You have a lot of exercises, you can't manage all those with ten compartments. So we usually have a single compartment, with multiple exercises at the same time. Then, because of an exercise, there are basically no secret classifications. At least, not at a higher level, at a basic level. So then you can do that together. But if it's really about missions, you have to divide it into separate compartments in principle. We will never run ten missions at the same time, but two or three would be able to. If nothing is left, then something will go down that has lower priority, and that's an exercise. ----- For instance take the entire *mobile IT organization*. What happens with a m*** network, you have to make sure that if say you go to Norway for an exercise, that those frequencies can be used. And that started to be more difficult to determine who was responsible for that, because it was more in telecommunications with all those mobile Internet connection capabilities. Then all of a sudden you need to go to S*** [military operation], it is necessary to support that operation, and in the Operations Room in Location B, for example, equipment should be used with all the required configurations. For example, somewhere at a transmission park we need to arrange something and then we need to arrange access, because there will be a lot of trouble if this does not happen. You must, of course, inform the user, we cannot just turn everything off just like that—that could lead to life-threatening situations. For example, the coast guard. For those kinds of things, we need to create all kinds of work places. We need to connect to NATO network, and there's a lot of pomp and circumstance around that. With security and everything related to that.
Urgent IT problem (during mission or exercise)	Then we will discuss what the impact of the problem is and whether it should be resolved immediately, whether it is possible to wait until tomorrow morning or after the weekend. If he indicates that it is so important now that someone is taken from home and put to work.

(Continued)

Table 6. (Continued)

Category of events that *trigger* emergency state	Exemplar quote
IS incident/problem in active networks (i.e. in the field)	For instance, Pete gets two days assigned and during those days he works for you. Unfortunately, we do not have that luxury, because those same people, for example, those in the "knowledge pool" that deliver those designs or settings to us—those are the same people as those who have to respond to incidents, and solve problems in active networks [i.e. networks used in war zones]. And resolving issues and incidents in active networks has a higher priority than our design support. I often have time-limited deadlines, a project must be completed before a certain time, but I can not claim any fixed resources to be able to meet those deadlines" [because resources might be shift to deal with incidents in active networks].
Serious IT issue that can cause security breach	Recently, we had a thing with the internet here at the port, so there is also the link to the ships. And at some point, the Internet connection is down, it is no longer working. The provider said there was a virus on the network, we immediately disconnected. Yes, all office buildings are also on that connection, many different users—so a virus can just pop up on the network, just like that. If you do not keep an eye on a scan program then it's bingo. So yes, probably in this case too. And yes ships were also stuck. So yes, look at the network, who is responsible for it now—is it MILIT, is it the Navy Command department? They picked it up at that time and then the provider went back to work and then our own maintenance guys found out we had an alternative line with the Internet. That's a private line, an ADSL line with the same provider. That was an alternate line for the internet and they could then connect. Because our people who are out there in S*** are also disconnected then, like everyone they communicate with out there in the G*** and places like that. And then it's full panic of course, if they can no longer communicate. So we set up the alternate line and had it all back online within 2 hours.
Life-threatening situation (can become an emergency if not addressed)	For example, somewhere at a transmission park we need to arrange something and then we need to arrange access, because there will be a lot of trouble if this does not happen. You must, of course, inform the user, we cannot just turn everything off just like that—that could lead to life-threatening situations. ------ When you're on your own somewhere . . . We also have contacts, for example, with officers who, for example, sit in Africa for some UN mission, who have a satellite system with a laptop and for the rest they are entirely self-appointed, if those call the service desk and feel that they are sent from pillar to post, you feel completely abandoned. You must have someone on the other side who knows and understands your situation and says "ok, I'm going to help you and I'll fix the problem and get a solution."

Table 7. Categories of events that *lead to* emergency state in traditional IT support function (Civit).

Category of events that *lead to* emergency state	Exemplar quote
Unknown IS incident that is turning into a problem	Then an incident is turned into a problem. A problem is something we need to research. That is brought to a specialist who will then dive into it. He neatly registers what he has found. He figures it out, together with others. Registers in that system what should happen and then an assignment to some software developers goes out that they need to change something.
Systems are down (i.e. "important IT unavailable for lots of people")	Only when things go down completely, yes. Then we will just work on until it's resolved. All of a sudden, we then call it a *calamity*. Sometimes that may be excessive but well, it helps the process. So if a piece infrastructure no longer works and important IT is unavailable for a lot of people, we just work on day and night until it's done. But the urgency is only when something really has failed. Only then will we find that important enough to work through the weekend.
A serious incident that becomes a calamity	Example of a cooler generator incident—see quote included in Table 3.
When a person cannot work due to IT failure/ high priority issue	High priority is when the help desk registers that a person can no longer work because of IT failure. We will try to solve that within 1 business day if he is completely unable to work. If the problem is less serious, like he doesn't have access to email: "yes, I can still work, I only miss 1 application . . ." Is not that urgent, it can take three days. And in itself, that's not so strange, because you can not solve everything within a day. But a person who can not work at all, must be given priority regardless of anything else. Always solve within 3 days. That's not so bad at all. But it does not always work within 3 days. And then someone is really suffering from it—a lot or a little less, but he has a lot of trouble. His work is hampered by this.
IS incident that escalates	When there's a disturbance, it's reported as an incident, and then they check whether they can solve it within a given amount of time and if they can't well then it goes to the IC: IC that is the Incident Coordinator. He then sees which unit it could concern, if it is hardware related then it will come to us and then they will order the replacement article. Or maybe it needs to be re-installed, we can do that remotely. If it can't be done remotely, then it goes through the planning office and ultimately to a field office somewhere. If hardware is related then it's always for us, at night we get our delivery. The appointment has been made with the customer and we go to the customer, we do our thing—either re-installing the PC or replacing it—and it's done. It can actually be anything. —- *Example of escalation*: If I get into the initiation phase, I agree to my contract, and then I claim people. And that's a big issue . . . Those people. We are planning here. I submit an application form, I put you in this project, I have skills A, B, C, and I have chosen informally, who can do it all, I put names, weeks and hours a week, I have to have it . . . Recently, I also had a serious escalation. I did not make any friends with it. Well, I don't have to—I have to get results. Planning said "no way." They also need these people here, so "no way." [. . .] In the end, they said "fine, we are going to prioritize it differently." And finally, I've got resources available this week, where first everybody said "no." Total "no." And as I said you always and everywhere get "no" for an answer. No time, no capacity. But as a project manager you are a representative of the customer. In this case, we do not know what kind of customer it is. Then you have to make sure it is settled. It's hell of a job. It's challenging.
IT request that cannot be accomplished in time (according to SLAs), therefore can escalate	I've asked to provide a facility that allows me to exchange encrypted email with the relevant vendor. And then I go to my IV manager because I'm also an employee in this company, so I go to my IV manager I say I need it. Well, he says, "you can do it yourself." No, I'm an employee of this company and I need it. So someone will provide this to me. I'm as well a supplier as a customer. And you see that the roles, they are not really clear to everyone. That I can both define requirements and provide stuff to other customers. And now the one thing that I need, I cannot provide myself. That comes from one of my colleagues. And then you are going down the official road by saying I'm making an application and then it will eventually be delivered through a process. That will be a non-standard request.
High-priority assignment due to resourcing issue	Then there is another new assignment that has high priority, so I have to drop a lot of work that I have now got out of my hands. Your customer needs to be informed that work is going to take time later has to be re-planned, so it costs a lot of capacity and you have to start working on that new job. At the moment that there are problems in the organization, there are always certain people who get called upon to fix things again. Often a very small group, that all of a sudden has to start arranging things. But at a certain point you see that within I & S there is a problem and something is really going wrong and something needs to be solved. Often, the same people are involved in solving this problem. I think that's in many organizations because (1) there are only a few people that have an overview of everything there is, especially with those kinds of systems—who can make a good analysis of where the problem actually is, and (2) the people with the technical expertise to actually solve those problems are even more scarce.

IS: Information Systems; SLA: service-level agreement.

and as there is a need to ensure that rival forces cannot access secret and classified information. Therefore, in Milit, the shift from normal to emergency operating conditions happens instantaneously. As the state of emergency is declared, military ranks are invoked and Milit switches to an operating mode according to the formal command and control framework guided by military principles.

Discussion

This study aimed to theorize about how organizational IT functions coordinate their work under different degrees of uncertainty in order to provide reliable IT services. Specifically, our empirical investigation focused on understanding how the coordination practices that IT functions employ to provide reliable IT services change when IT incidents cause a change from normal (i.e. "business-as-usual") to emergency conditions. We conceptualized IT functions' responses to an emergency as a "shift" of coordination practices and analyzed how such a shift actually happens, leading to change in coordination practices employed under different levels of uncertainty.

Coordination dynamics in IT support functions: toward a process view

We theorize coordination in IT support functions as a process that unfolds over time through interactions between the four underlying coordination practices: *prioritizing tasks, following procedures, using roles and responsibilities*, and *utilizing networks*. Nevertheless, each practice may be enacted in various ways, that is, through a repertoire of different coordinative activities (summarized in Tables 4 and 5). The nature of the activities constituting each practice (i.e. whether they are prescribed or ad hoc) signals whether a practice supports *structured* or *improvised* coordination modes (Faraj and Xiao, 2006; Kotlarsky et al., 2014), as we discuss later in this section. Analyzing how the shift from normal to emergency operating conditions happens helps to understand the differences in the level of preparedness of an IT support function to respond to emergencies and restore reliable IT services.

When an event triggers change in the operating conditions from normal to emergency, coordination practices used under normal conditions become unsuitable, which prompts the IT function to switch to alternative ways of coordinating. In the fast-response IT support function, this alternative consists of a pre-defined "emergency" set of practices, while in the traditional IT support function alternative practices are largely based on improvisation (see Table 8).

Figure 3 captures coordination as a process that, when affected by changes in operating conditions, shifts from a normal to an emergency state and then returns to business-as-usual after the emergency has been addressed and reliable IT services have been restored. This high-level process view highlights the difference in the time-line between traditional versus fast-response IT support functions in the occurrence of such a shift. Furthermore, this view also helps identify the key characteristics of the shift that leads the traditional IT function to pursue improvised coordination, while the fast-response IT function resorts to emergency coordination practices. As events originating in an external environment (e.g. changes in the geo-political situation) or internal reasons (e.g. unexpected equipment failure or critical organizational missions) affect the functioning of the organization, the IT function is put under pressure to resolve the issue. In response to emergency situations, the IT function engages in coordination practices that are suitable to address these urgent needs. These practices are inter-related either by *defining, following, deciding*, or *prescribing* another practice (as discussed in episodes 1 and 2 and illustrated by different configurations of coordination practices that both IT functions enact in normal operating conditions and when dealing with emergencies in Figures 1 and 2).

Comparing coordination dynamics in traditional and fast-response IT support functions

Analyses of the interactions between coordination practices (illustrated in Figures 1 and 2) demonstrate different dynamics between coordination practices under different operating conditions, resulting in different configurations—one that captures coordination during *normal operating conditions* (e.g. Figure 1) and the other that reflects how work in an IT support function is coordinated in the case of an *emergency* (e.g. the two diagrams in Figure 2). Essentially, the analyses presented in the previous sections of this article indicate that, in terms of coordination, a fast-response IT function reacts quite differently to a shift to an emergency state than a traditional IT function. A fast-response IT function is more prepared for emergencies, as it has a set of well-structured mechanisms that define how work is to be coordinated under such circumstances. Employees in such IT functions are familiar with both sets of coordination practices (i.e. business-as-usual as well as emergency practices) and are trained to switch between the two when operating conditions change. In particular, when a fast-response IT function faces an emergency, the already formal ways of coordinating work become even more formal and tight, removing any possible ambiguity that could potentially harm the ability of this IT function to achieve its goals. Informal networks are no longer utilized, and higher ranks define the priority of tasks which in turn defines how work should be coordinated: guided by formal protocols, procedures, and codes of conduct. Overall, as illustrated in Figures 1 and 2, the inter-relationships between different coordination practices remain largely the same when operating conditions in a fast-response IT function shift from normal to emergency, but the enactment of each practice (which takes place through a

Table 8. Main characteristics of the coordination process under normal and emergency operating conditions in traditional and fast-response IT support functions.

	Normal conditions	Emergency conditions
Traditional IT support function	Largely structured coordination practices Personal networks are used to speed things up	Largely improvised and informal coordination practices aimed at resolving the emergency (as "normal" procedures and protocols are not able to address emergency situations and there are no/minimal emergency procedures in place) Personal networks are dominant, which (+) allows for ad hoc collaborations, but (–) may result in anarchy
Fast-response IT support function	Largely structured coordination practices Informal networks rely on joint experiences and visual indicators (i.e. uniform) indicating similar experiences	Highly structured and formal coordination practices aimed at achieving best performance (these practices rely on a specific set of "emergency" protocols, procedures, and other activities that are evoked in emergency situations and followed strictly) Informal networks cease to exist which means that (+) coordination is highly efficient, but (–) no room for discussion

(+) and (–) in this table stands for pros and cons (accordingly).

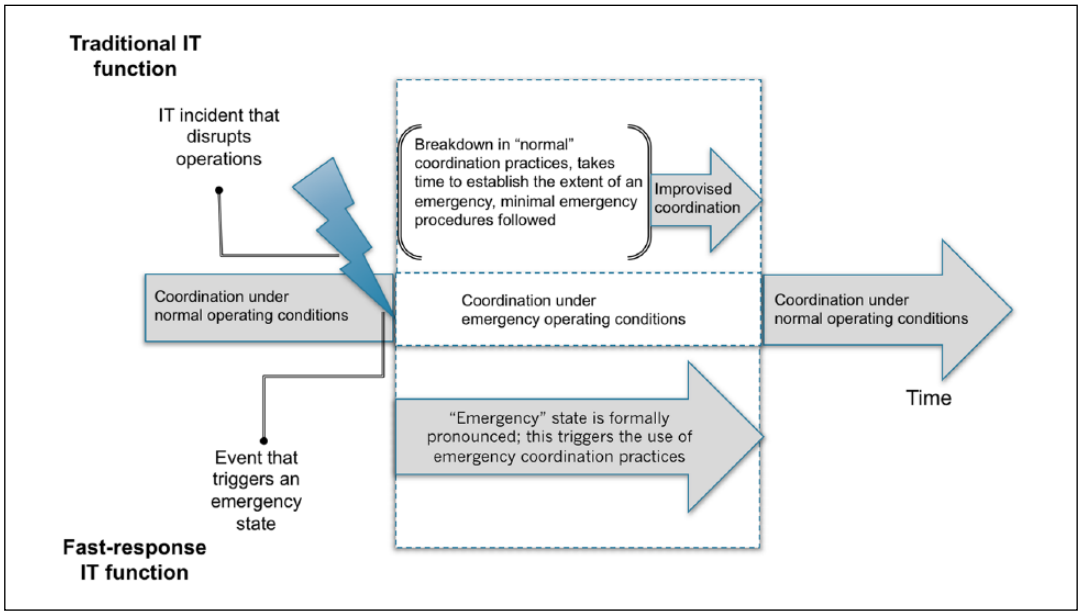

Figure 3. Coordination process in traditional and fast-response IT support functions.

portfolio of specific coordinative activities associated with each practice) changes significantly, as the set of activities for normal conditions is replaced by the set of activities for emergency conditions (see the activities listed in Table 5).

On the contrary, when a traditional IT function faces an emergency situation, structures and formalities (procedures, rules, and regulations) that define how work is coordinated under normal conditions fall apart. An incident or breakdown that leads to an emergency requires a re-assessment of priorities and amplifies the need to remove all formal organizational boundaries to allow efficient coordination in order to resolve the emergency and restore reliable IT services. Informal networks become the main driver of coordination, as individuals rely extensively on their personal networks to find relevant experts and bring them together in an attempt to resolve the emergency. As formal coordination mechanisms largely dissolve, there is space for creativity and improvisation in coming up with solutions for the crisis. Having a *carte blanche*, for example, is one way to legitimize the lack of structure and formal approaches for coordinating work. In Table 8, we summarize the main characteristics of the coordination process where we distinguish between normal and emergency operating conditions in traditional and fast-response IT support functions.

As depicted in Table 8, in the traditional IT support function, a *largely structured* way of coordinating work under normal conditions shifts to *largely improvised* and informal when faced with an emergency. In contrast, in the fast-response IT support function, the *largely structured* approach to coordination that we observed in normal situations changes to *highly structured* and formal under emergency conditions.

Explaining different coordination dynamics: the nature of an emergency and integrating conditions for coordination

An important conclusion that we can draw from the previous discussion is that traditional IT functions are less prepared for emergencies than fast-response ones. In this section, we integrate our findings with the literature to explain this phenomenon in more detail and explore how IT support functions in traditional organizations could shape their coordination process in a way that is better prepared for responding to emergency conditions so that reliable IT services can be restored after emergencies occur.

First, we need to consider how IT functions in different types of organizations perceive an "emergency." We defined an emergency operating condition as "a situation that (1) contains pervasive uncertainty; (2) creates pressure for quick execution; and (3) can have negative consequences such as additional costs or creates a danger of severe physical harm." The fast-response IT support function in our study is similar to SWAT and police teams as studied by Okhuysen and Bechky (2009) and Schakel et al. (2016) in the sense that it had mechanisms in place to adapt coordination practices to the requirements of an emergency. In our study, the IT function supporting the Military division of the MoD was prepared for dealing with new, uncertain, and unexpected situations through *formalization*. The traditional IT function, on the other hand, was clearly not prepared for surprises, and any "discrepant IT events" (de Guinea and Webster, 2013) that would fall outside what would be considered within this function as "normal accidents" (Perrow, 1999) or typical IT projects could create a challenge for coordinating IT work. In this function, the lack of structured and pre-defined coordination practices for emergency situations was compensated for by having specific crisis manager and escalation manager roles that were only invoked in an emergency situation. As there were no established structures or processes on which these roles could rely, however, their actions were by definition ad hoc and improvised, without sufficient opportunity for adapting "normal" coordination practices to the requirements of emergency situations.

These findings are in line with Bigley and Roberts' (2001) conclusions that traditional systems cannot be relied on when faced with an emergency situation. In response to such a situation, a traditional organization tries to achieve flexibility through improvisation and temporary arrangements. For instance, in the analysis of the Mann Gulch disaster, Weick (1993) highlighted the importance of role improvisations. He argued that "the collapse of role systems need not result in disaster if people develop skills in improvisation and bricolage" (p. 639). However, it is important to note that the traditional IT function in our study had to *improvise* because it did not have a choice, and not because it had an inherent ability to engage in organizational improvisation (Bechky and Okhuysen, 2011).

Interestingly, the way that the fast-response IT support function in our study responded to emergencies is not entirely in line with how, for instance, the SWAT team in Bechky and Okhuysen's (2011) study reacted by improvising or relying on "organizational bricolage" practices such as role-shifting, reorganizing routines, and reassembling their work in response to specific situational demands. Instead, the fast-response IT function in our study relied on *formalization* through bureaucratic mechanisms such as command and control to cope with emergencies, essentially exhibiting some similarity to what Bigley and Roberts (2001) called an Incident Command System-based organization, providing the ability to "capitalize on command and control benefits of bureaucracy, while avoiding or overcoming the considerable tendencies towards inertia" by, for instance, leaving room for *constrained* improvisation (Bigley and Roberts, 2001: 1281).

A possible explanation for the differences between fast-response and traditional IT support functions in terms of the "readiness" of their coordination process for emergencies can be provided by analyzing the differences in *integrating conditions* for coordination as proposed by Okhuysen and Bechky (2009). These authors argued that successful coordination is likely if (some or all of) three integrating conditions are met: accountability (who is responsible for specific elements of the task?), predictability (what subtasks make up larger tasks and in what order will they be performed?), and common understanding (what is the shared perspective on the task, and how does an individual's work fit into the whole?). These integrating conditions for coordination of work are relevant to knowledge-intensive work in IT support function.

Specifically, the *accountability* condition is met when members of IT support function are clear regarding responsibilities of interdependent parties (including their own), which helps to set the right expectations. *Predictability* is achieved when organizational members are able to anticipate when and how interdependent actors would act, which allows individuals to plan and perform their own actions. Finally, *common understanding* is high when interdependent actors share knowledge of the whole IT project or issue that they are contributing to: what needs to be done, how it is to take place, the overall goals and objectives. Understanding a broader context and having a shared perspective helps individuals to fit their work within the whole.

As we have observed in our study, four coordination practices—using roles and responsibilities, prioritizing tasks, utilizing networks, and following procedures—contribute toward creating these integrating conditions for coordinating of work when both traditional and fast-response IT functions operate under normal conditions. Specifically, *roles and responsibilities* facilitate accountability; *priority of tasks* and *procedures* help to predict what should happen next and how it should happen; and *networks*, which rely on familiarity between organizational members, increase common understanding between individuals.

Okhuysen and Bechky (2009) viewed integrating conditions for coordination as an outcome of coordinative efforts which can be accomplished through a variety of mechanisms that combine formal planned mechanisms and emergent interactions. In line with this view, we can explain why, despite a variety in the repertoire of coordinative actions that the fast-response and traditional IT support functions in our study employed to coordinate their work (depicted in Tables 4 and 5), both functions were able to meet the three integrating conditions to support coordination under normal operating conditions. Among the four coordination practices, *utilizing networks* introduced an informal element supporting emergent interactions based on familiarity, which is considered to be a key for achieving predictability and common understanding. Where, in the traditional IT function, familiarity relied on inter-personal relationships and past experiences of working together, familiarity in the fast-response IT function was embodied in the military uniform—as color of the uniform and rank implied certain experiences which colleagues could easily interpret and associate with. Furthermore, the fast-response IT function had a stronger social identity due to the fact that most employees were military personnel, which facilitated coordination by promoting a thorough consideration of another's knowledge (Kane, 2010).

However, an event that triggered an emergency situation eroded integrating conditions for coordinating work that were appropriate for coordinating under normal conditions. Despite the fact that both IT functions enacted a different set of coordination mechanisms when dealing with emergencies, the fast-response IT function was able to re-create integrating conditions through the use of alternative (emergency-specific) coordinative activities such as relying on military rank and associated hierarchy, enacting emer-gency procedures and relying on the formal network. Accountability was enforced through the formal hierarchy and regimented nature of the unit, and common understanding was maintained by the regiment following military principles captured in the code of conduct and known to all personnel, which in turn helped to manage expectations, to anticipate actions of others, and to increase predictability by defining the order. As noted above, changes in coordination practices we have identified in the fast-response IT function resemble an Incident Command System (Bigley and Roberts, 2001) invoked in response to an emergency. Such a system ensures that the integrating conditions for coordination are met, as it leaves no room for doubt about who is responsible for what, what the shared principles are, and what actions are to be expected.

The traditional IT function, however, struggled to re-create integrating conditions to support coordination under emergency conditions. Two emergency-specific roles—escalation and crisis managers—seemed to be insufficient to re-create accountability as all other "normal" roles dissolved, which led to situations where the "one who shouts the loudest" was able to attract the attention of top management and determine the prioritizing of tasks. Replacing formal networks with informal ones increased the reliance on familiarity embodied in these informal networks as one of the main coordination mechanisms (e.g. to negotiate responsibilities when dealing with an emergency and decide on how to proceed in the absence of suitable formal procedures). Thus, relying on who knows whom and what they know about each other became the main driver behind the improvised (ad hoc) efforts to accomplish coordination in this IT function. This limited the possibility to achieve common understanding and predictability to small groups of people who were familiar with each other and therefore connected through informal networks.

To conclude, we believe that the integrating conditions for coordination help us to understand whether (or not) an IT support function is prepared to face the unexpected and deal with "discrepant IT events" (de Guinea and Webster, 2013) and could help traditional IT functions to improve their ability to ensure reliable provision of IT systems and services under emergency conditions.

Theoretical implications

Our research offers significant implications for theory. First and foremost, it contributes to the literature that addresses problems facing the IT function (Rai, 2016), a topic which is central to the IS research agenda. At present, theoretical developments advancing our knowledge about the role and contribution of the IT function are at a nascent stage, focusing on the way the IT function combines different roles in order to meet business needs—varying from providing reliable systems to leading business innovation (Guillemette et al., 2017; Guillemette and Paré, 2012; Tarafdar and Tanriverdi, 2018)—and the organizing challenges that emerge in relation to this combination of roles (Gregory et al., 2015; Haffke et al., 2017; Kude et al., 2017; Peppard, 2018). Our study contributes to this stream of IS literature by specifically focusing on how the IT function responds to incidents to restore reliable service provision and by offering a more refined understanding of the *process* through which IT functions coordinate work in order to support organizational IT needs (Guillemette and Paré, 2012) and address the problem of reliability of IS (Butler and Gray,

2006). Our unique contribution is in theorizing coordination in the IT support function as a dynamic process that changes as an IT function is confronted with emergency conditions. Specifically, we (1) conceptualize coordination in IT support function as a process that unfolds over time through interactions between the four underlying coordination practices: prioritizing tasks, following procedures, using roles and responsibilities, and utilizing networks, and (2) show how these coordination practices that IT functions employ to provide reliable IT services change when IT incidents cause a shift from normal (i.e. "business-as-usual") to emergency conditions.

This brings to the fore the need to take into account changes in the conditions under which the IT function is expected to provide support to the organization. In an era when technologies have become a backbone and life blood of most organizations, IS incidents of different severity disrupt business-as-usual and often put immense pressure on the IT support function. Therefore, being prepared for emergencies means being able to mobilize and adjust the coordination of IT work to provide reliable IT services even when faced with emergency situations. Capturing the shift in coordination between normal and emergency operating conditions depicted in our process view (Figure 3) is an important aspect of our theoretical contribution, as it highlights that there is a variation between how different IT support functions respond to events that disrupt "business-as-usual." Moreover, categorizing a variety of events that are considered as *triggering* an instant shift to an emergency state (in fast-response IS function) or eventually (or very likely) *leading to* emergency (in traditional IT functions) is a small but novel contribution that is relevant to our understanding of IS incidents.

Our second contribution is in distinguishing between IT functions supporting traditional and fast-response organizations and demonstrating that while there is a single baseline depicting coordination in both types of IT functions under normal operating conditions, IT functions in two different types of organizations respond to emergencies differently, as captured in the process view (Figure 3). This contributes to the stream of research on different approaches that IT functions have toward handling incidents and achieving reliable IT performance. Butler and Gray (2006) distinguish two strategies that IT functions follow to achieve reliable performance: routine-based reliability versus mindfulness-based reliability, implying two different ways of handling IS incidents. Routine-based reliability implies a focus on "repeatable packages of decision rules and associated actions" (Butler and Gray, 2006: 214) to handle incidents, with a focus on a reduction of errors, and on preventing and preparing for incidents. "Mindfulness-based reliability," however, implies a more agile and responsive way of handling incidents, with a focus on resilience: the ability to cope with incidents as they arise, based on quick detection and analysis of incidents, and the capacity to make quick and accurate decisions in response to such incidents. Our study indicates the importance of considering the nature of the organization the IT function serves (traditional vs fast-response) and the operating conditions (business-as-usual vs emergency) to explain how an IT function most effectively responds to a shift from business-as-usual to emergency operating conditions: where the routine-based reliability approach that characterizes the IT function in the traditional organization falls apart and leads to what Butler and Gray call "mindless behavior" (being unable to handle incidents that do not fall into the established categories and strategies), an IT function in a fast-response organization is much more geared toward resilience and flexibility within the constraints of a clear command and control structure.

Practical implications

Clearly, a non-military IT function cannot become as strict as a military one when it comes to relying on ranks and formal hierarchy. However, an IT function can consider other ways to re-create accountability, predictability, and common understanding, such as expanding "emergency" roles beyond emergency and crisis managers to include some supporting inter-disciplinary (e.g. cross-departmental) roles to act as boundary spanners (Gittell, 2002) and to help in channeling relevant knowledge between individuals and groups involved in dealing with the emergency. In particular, IT functions in fast-response organizations, such as A&E units in hospitals or air traffic control centers, should consider what can they learn from IT functions supporting military types of organization. For example, when a patient is on the operating table, supporting IS are critical, just like when a platoon is in a combat zone. Beyond hospitals, other professional fields such as air traffic control, or banking systems, would find these results significant for their practice.

Given the increasing severity of IS incidents and cybercrime (as illustrated in the opening examples), today more considerations should be given to preparing traditional IT functions for "surprises." Moreover, increasingly severe weather (more severe, more often) on a global scale will amplify the frequency of critical IS outages, which means that IT functions in most organizations will be put under pressure to provide reliable IT services despite emergency conditions.

Traditional IT support functions are more likely to be significantly affected by events or situations that disrupt business-as-usual in their organizations if they do not have in place structures to fall back on in the cases of emergencies. A small IS incident may cause serious disruption and become a "calamity" (as an interviewee in Civit put it) if not contained and addressed quickly. In his analysis of the Mann Gulch disaster, Weick (1993) stressed,

> The recipe for disorganization in Mann Gulch is not at all that rare in everyday life. The recipe reads, thrust people into

> unfamiliar roles, leave some key roles unfilled, make the task more ambiguous, discredit the role system, and make these changes in a context in which a small event can combine into something monstrous. (p. 638)

In the digital era we live in, in addition to "normal" IS incidents and failures, any IT function is constantly under a cybersecurity threat. Therefore, to ensure reliability of IT in their organization, traditional IT functions could consider some of activities used in fast-response IT function (e.g. from those listed in Table 5) to establish more structured and formalized approach to coordination when dealing with emergencies.

Limitations and further research

This research is not free from limitations. First of all, our study took place in a particular kind of organization: a military organization. On one hand, this provided the ideal setting to compare IT functions that supported a traditional and a fast-response organization within a similar setting. Both bureaucracy and fast-response work are fundamental characteristics of military work, and the fact that ITSO had specific divisions for IT support for both these parts of the organization meant we could compare these IT functions without additional organizational differences coming into play—both Civit and Milit are part of the same larger organization, after all. On the other hand, some of our findings may be specific for military organizations and are perhaps less generalizable to other IT functions. For example, the command-and-control logic that was especially manifest in how Milit responded to emergencies may be inherent to the military character of that organization, and it could be that we would not find this mechanism so prominently in other IT functions in fast-response organizations. Also, in a military organization, the uniform plays an important role in coordination because it evokes common experiences and provides visual indication of ranks. IT functions supporting other fast-response organizations (e.g. hospitals, fire brigades, or police) may not have such uniforms to rely upon (e.g. some policemen are dressed as civilians to remain under cover). Furthermore, in some organizations, the distinction between fast-response and traditional IT support may not be a clear cut. For example, in hospitals, fast-response IT support is required in A&E and in operation theaters (for surgeries), while some departments (e.g. outpatients) may not need same degree of urgency in IT support. Thus, future research should extend the investigation of how IT functions respond to a shift from "business as usual" to an emergency state beyond military organizations and study if similar patterns exist in other organizations that combine bureaucracy and fast response. Such studies could look into tensions associated with different degrees of urgency in the required IT support, and how the IT support function is dealing with these tensions. Investigating the link between IS incidents of various degrees and coordinative actions could be another avenue to explore in the future research.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Bart van den Hooff https://orcid.org/0000-0002-8880-3910

Notes

1. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack. Following this first attack on UK hospitals, ransomware spread to many countries around the world https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs
2. Jarvenpaa and Majchrzak (2008) defined *dialogic practices* as "semi-structures that describe rules of conversation" (pp. 262–263). They referred to *rules* of dialogic practices offered by Boland et al. (1994) that include "discussing sources of knowledge, encouraging knowledge emergence, comparing multiple perspectives, keeping knowledge indeterminant to be repeatedly revised in response to new information, and structuring discussions to move between summary-level knowledge and detailed analysis" (pp. 262–263).
3. As Langley et al. (2013: 7) explained:

> Comparing distinct cases is not however the only way to achieve replication. It is a common misconception that longitudinal case studies represent "samples of one." However, it is important to note that the sample size for a process study is *not* the number of cases, but the number of *temporal observations*. Depending on how researchers structure their analysis, the number of temporal observations in a longitudinal study can be substantial.

References

Baskerville R, Spagnoletti P and Kim J (2014) Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management* 51(1): 138–151.

Basselier G and Benbasat I (2004) Business competence of information technology professionals: Conceptual development and influence on IT-business partnerships. *MIS Quarterly* 28(4): 673–694.

Bechky BA and Okhuysen GA (2011) Expecting the unexpected? How SWAT officers and film crews handle surprises. *Academy of Management Journal* 54(2): 239–261.

Bigley GA and Roberts KH (2001) The incident command system: High reliability organizing for complex and volatile task environments. *Academy Management Journal* 44(6): 1281–1299.

Boland RJ Jr, Tenkasi RV and Te'Eni D (1994) Designing information technology to support distributed cognition. *Organization Science* 5(3): 456–475.

Bouty I, Godé C, Drucker-Godard C, et al. (2012) Coordination practices in extreme situations. *European Management Journal* 30(6): 475–489.

Butler BS and Gray PH (2006) Reliability, mindfulness, and information systems. *MIS Quarterly* 30(2): 211–224.

Carlile P (2004) Transferring, translating and transforming: An integrative framework for managing knowledge across boundaries. *Organization Science* 15(5): 555–568.

de Guinea AO and Webster J (2013) An investigation of information systems use patterns: Technological events as triggers, the effect of time, and consequences for performance. *MIS Quarterly* 37(4): 1165–1188.

Faraj S and Xiao Y (2006) Coordination in fast-response organizations. *Management Science* 52(8): 1155–1169.

Farrell T, Osinga F and Russell J (2013) *Military Adaptation in Afghanistan*. Stanford, CA: Stanford University Press.

Gioia DA, Corley KG and Hamilton AL (2013) Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods* 16(1): 15–31.

Gittell JH (2002) Coordinating mechanisms in care provider groups: Relational coordination as a mediator and input uncertainty as a moderator of performance effects. *Management Science* 48: 1408–1426.

Gregory RW, Keil M, Muntermann J, et al. (2015) Paradoxes and the nature of ambidexterity in IT transformation programs. *Information Systems Research* 26(1): 57–80.

Guillemette MG and Paré G (2012) Towards a new theory of the contribution of the IT function in organizations. *MIS Quarterly* 36(2): 529–551.

Guillemette MG, Mignerat M and Paré G (2017) The role of institutional work in the transformation of the IT function: A longitudinal case study in the healthcare sector. *Information & Management* 54(3): 349–363.

Haffke I, Kalgovas B and Benlian A (2017) Options for transforming the IT function using bimodal IT. *MIS Quarterly Executive* 16(2): 101–120.

Jarvenpaa SL and Majchrzak A (2008) Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. *Organization Science* 19(2): 260–276.

Jia R and Reich BH (2013) IT service climate, antecedents and IT service quality outcomes: Some initial evidence. *Journal of Strategic Information Systems* 22(1): 51–69.

Kane AA (2010) Unlocking knowledge transfer potential: Knowledge demonstrability and superordinate social identity. *Organization Science* 21(3): 643–660.

Kellogg KC, Orlikowski WJ and Yates J (2006) Life in the trading zone: Structuring coordination across boundaries in postbureaucratic organizations. *Organization Science* 17(1): 22–44.

Kettinger WJ and Lee CC (1994) Perceived service quality and user satisfaction with the information services function. *Decision Sciences* 25(5–6): 737–766.

Kotlarsky J, Scarbrough H and Oshri I (2014) Coordinating expertise across knowledge boundaries in offshore-outsourcing projects: The role of codification. *MIS Quarterly* 38(2): 607–627.

Kude T, Lazic M, Heinzl A, et al. (2018) Achieving IT-based synergies through regulation-oriented and consensus-oriented IT governance capabilities. *Information Systems Journal* 28(5): 765–795.

Langley A (1999) Strategies for theorizing from process data. *Academy of Management Review* 24(4): 691–710.

Langley A, Smallman C, Tsoukas H, et al. (2013) Process studies of change in organization and management: Unveiling temporality, activity, and flow. *Academy of Management Journal* 56(1): 1–13.

Majchrzak A, Jarvenpaa SL and Hollingshead AB (2007) Coordinating expertise among emergent groups responding to disasters. *Organization Science* 18(1): 147–161.

Miles MB and Huberman AM (1994) *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks, CA: SAGE.

Okhuysen GA and Bechky BA (2009) Coordination in organizations: An integrative perspective. *The Academy of Management Annals* 3(1): 463–502.

Peppard J (2003) Managing IT as a portfolio of services. *European Management Journal* 21(4): 467–483.

Peppard J (2018) Rethinking the concept of the IS organization. *Information Systems Journal* 28(1): 76–103.

Perrow C (1999) *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Rai A (2016) The MIS quarterly trifecta: Impact, range, speed. *MIS Quarterly* 40(1): iii–x.

Sambamurthy V and Zmud RW (2000) Research commentary: The organizing logic for an enterprise's IT activities in the digital era—A prognosis of practice and a call for research. *Information Systems Research* 11(2): 105–114.

Schakel J-K, van Fenema PC and Faraj S (2016) Shots fired! Switching between practices in police work. *Organization Science* 27(2): 391–410.

Strauss AL and Corbin JM (1998) *Basics of Qualitative Research*. Thousand Oaks, CA: SAGE.

Tarafdar M and Tanriverdi H (2018) Impact of the information technology unit on information technology-embedded product innovation. *Journal of the Association for Information Systems* 19(8): 716–751.

Umble EJ, Haft RR and Umble MM (2003) Enterprise resource planning: Implementation procedures and critical success factors. *European Journal of Operational Research* 146(2): 241–257.

Venters W, Oborn E and Barrett M (2014) A trichordal temporal approach to digital coordination: The sociomaterial mangling of CERN grid. *MIS Quarterly* 38(3): 927–949.

Weick KE (1993) The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly* 38(4): 628–652.

Author biographies

Julia Kotlarsky is Professor of Technology and Global Sourcing at the University of Auckland Business School in New Zealand. Her research interests revolve around technology sourcing and innovation in knowledge-intensive business services, coordination in complex and dynamic organizational settings, and more recently, studying interface between artificial intelligence technologies and humans. Her work was published in numerous journals including *MIS Quarterly, Journal of Management Information Systems, Journal of Strategic Information Systems, Wall Street Journals* and others. Her book "*The Handbook of Global Outsourcing and Offshoring*" is widely used by academics and practitioners. She is co-founder of the annual Global Sourcing Workshop (www.

globalsourcing.org.uk). Julia serves as a Senior Editor for the *Journal of Information Technology* and a former Associate Editor for *MIS Quarterly*.

Bart van den Hooff is Professor of Organizational Communication and Information Systems at the KIN Research Group, School of Business and Economics, Vrije Universiteit Amsterdam. His research focuses on the management of ICT for digital innovation – from managing IS complexity to IS development and implementation, and from the use of mobile devices to managing the IT function. His work has been presented at international conferences and published in (among others) *MIS Quarterly, Journal of Management Studies, Communication Research, Human Communication Research, Organization Studies, European Journal of Information Systems,* and the *Journal of Information Technology*.

Leonie Geerts is Director of Business Operations and Organizational Development at Logius, part of the Ministry of the Interior and Kingdom Relations in the Netherlands. Before she worked at the intersection of IT and Business Operations at several governmental organizations, and at the KIN Research Group, School of Business and Economics, Vrije Universiteit Amsterdam. Her work has been presented at international conferences and published in Communication Research and the International Military Leadership Association.

Appendix A

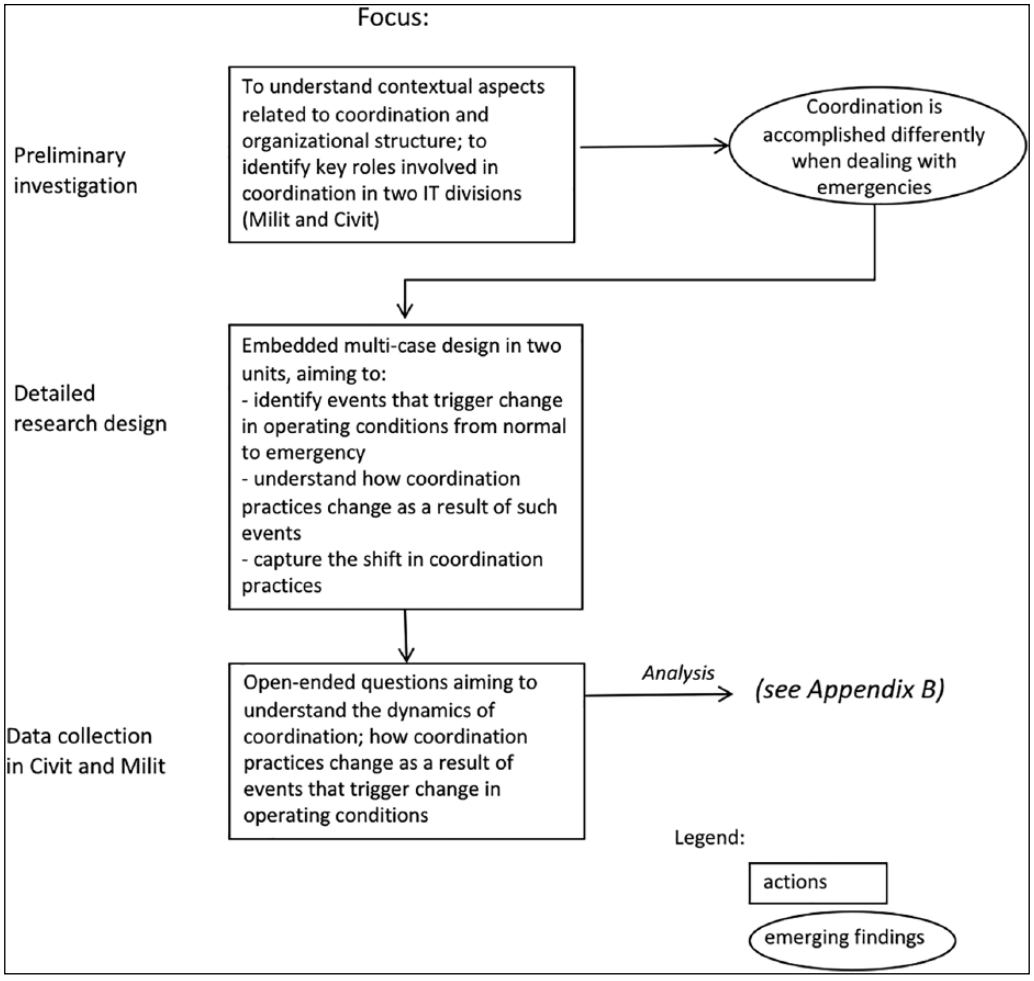

Figure 4. Research design and data collection process (schematic).

Appendix B

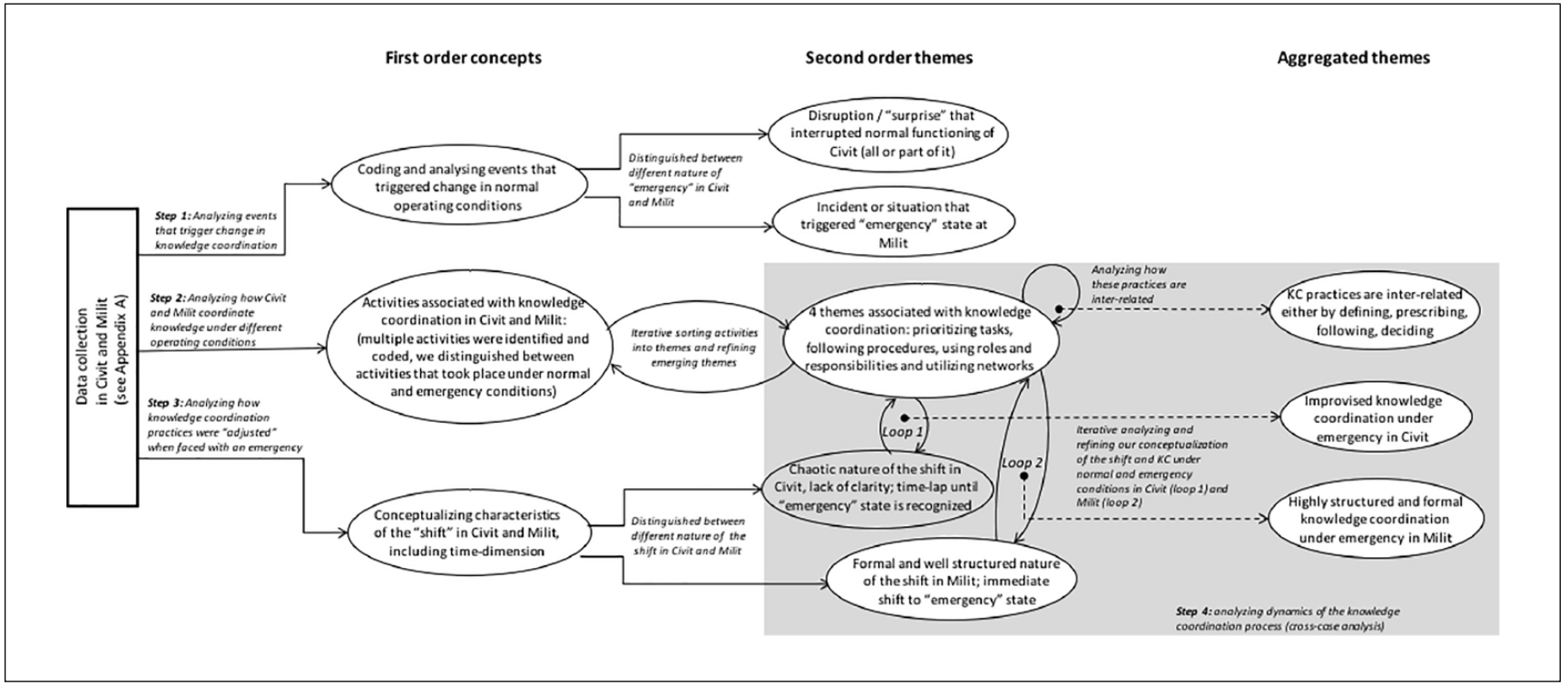

Figure 5. Data analysis process.

Steps 1–3 in data analysis are along arrows they illustrate, and step 4 (cross-case analysis) is illustrated in the gray area.

Appendix C

Table 9. Interviewee details.

Interviewee details					
No.	IT function	Gender	Functional role	Civilian/Military	Interview duration
1	Civit	M	Senior project desk employee	Civilian	0:52
2	Civit	M	Process manager	Civilian	0:49
3	Civit	M	Unit manager	Civilian	1:01
4	Civit	M	Product group manager	Civilian	0:57
5	Civit	M	Senior process manager	Civilian	1:08
6	Civit	M	Product manager	Civilian	1:02
7	Civit	M	Delivery manager	Civilian	1:01
8	Civit	M	Advisor	Civilian	0:56
9	Civit	M	IT manager	Civilian	0:54
10	Civit	M	Senior advisor	Military	1:21
11	Civit	M	Senior process owner	Civilian	1:09
12	Civit	F	Project quality assurance employee	Civilian	0:48
13	Civit	M	Head of Cluster	Civilian	0:55
14	Civit	M	Senior program manager/Escalation manager	Military	2:20
15	Civit	M	Commander	Civilian	1:18
16	Civit	M	System architect	Civilian	0:50
17	Civit	M	Senior IT maintenance	Civilian	1:03
18	Civit	M	Senior program manager	Civilian	1:45
19	Civit	F	Senior project secretary	Civilian	0:46
20	Civit	F	Transition manager	Civilian	1:01
21	Civit	M	Senior project leader	Civilian	0:56
22	Milit	M	Senior project manager	Military	1:17
23	Milit	M	Head of Internal Affairs	Civilian	0:57
24	Milit	M	Head of National Networks	Military	1:01
25	Milit	M	Head of Client Contact Point	Military	0:53
26	Milit	M	Head of Knowledge Pool	Military	2:20
27	Milit	F	Quality manager	Civilian	1:10
28	Milit	M	Senior technical specialist	Civilian	1:05
29	Milit	M	Head of Controlling Department	Military	1:10
30	Milit	M	Head of Information Security	Military	1:00
31	Milit	M	Commander	Military	1:09
32	Milit	M	Head of Operations Room	Military	1:04
33	Milit	M	Head of Resource Planning/Configuration manager	Military	0:48